ROUTLEDGE

ANDREA MONTI AND RAYMOND WACKS

NATIONAL SECURITY IN THE NEW WORLD ORDER

GOVERNMENT AND THE TECHNOLOGY OF INFORMATION

NATIONAL SECURITY IN THE NEW WORLD ORDER

This important new book explores contemporary concerns about the protection of national security. It examines the role, influence, and impact of Big Tech on politics, power, and individual rights. The volume considers the manner in which digital technology and its business models have shaped public policy and charts its future course.

In this vital text for legislators and policymakers, Andrea Monti and Raymond Wacks draw on several case studies to analyse the changing nature of national security and revisit the traditional idea of the sovereignty of the State. They highlight some of the limitations of the conventional understanding of public policy, national security, and the rule of law to reveal the role of digital technology as an enabler as well as discriminator in governance and social disorder. Further, the chapters in the book explore the tenuous balance between individual freedom and national security; the key role of data protection in safeguarding digital data; Big Tech's appropriation of national security policy; the debate relating to data-gathering technologies and encryption; and offers an unsettling answer to the question 'what is a leak?'

A stimulating read, this key text will be of immense interest to scholars of politics, cyberculture, and national security, as well as to policy analysts, lawyers, and journalists.

Andrea Monti is an Italian lawyer, journalist, and academic, whose expertise ranges from biotechnology to privacy and high-tech law. He taught Public Order and Security at the Gabriele d'Annunzio, University of Chieti, Italy, where he is now an Adjunct Professor of Digital Law. Over the last two years, he delivered lectures as part of the Italian State Police training programmes. He has published several papers on bio-information, computer forensics, technology, and public order, as well as books on computer hacking. His most recent publications are *Protecting Personal Information: The Right to Privacy Reconsidered* (2019), and *COVID-19 and Public Policy in the Digital Age* (2021), with Raymond Wacks.

Raymond Wacks is Emeritus Professor of Law and Legal Theory at the University of Hong Kong, China. He has published more than 20 books which have been translated into a dozen languages. His works include *Personal Information: Privacy and the Law*; *Privacy and Media Freedom*; *Privacy: A Very Short Introduction*; and *Law: A Very Short Introduction*. His most recent publications are *Protecting Personal Information: The Right to Privacy Reconsidered* (2019), and *COVID-19 and Public Policy in the Digital Age* (2021), with Andrea Monti. The sixth edition of his *Understanding Jurisprudence: An Introduction to Legal Theory* was published in 2021, as was *The Rule of Law Under Fire?*

NATIONAL SECURITY IN THE NEW WORLD ORDER

Government and the Technology of Information

Andrea Monti and Raymond Wacks

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2022
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested for this book

ISBN: 978-0-367-40801-5 (hbk)
ISBN: 978-0-367-80971-3 (pbk)
ISBN: 978-0-367-80977-5 (ebk)

DOI: 10.4324/9780367809775

Typeset in Sabon
By Deanta Global Publishing Servies, Chennai, India

Andrea Monti dedicates this book to his family and to the memory of his mentor, the late Giancarlo Livraghi. He wishes to thank Hiroshi M[illegible]ta of Chuo University, Andrea Ortolani of Keio Universit[illegible]rgio Colombo of Nagoya University, Mariarosaria Taddeo of the Oxford Internet Institute at the University of Oxford, Gianfranco Purpura of the University of Palermo, Commander Massimilano Dosi of the Italian Navy, Carlo Disma, analyst at Rivista Italiana Difesa, and Francesco Di Maio, Head of Corporate Security at ENAV, the Italian air navigation service provider.

Raymond Wacks is grateful to his wife Penelope for her tolerance over half a century, and to Archie and Bertie for occasionally permitting him access to his keyboard.

We are, yet again, grateful to Aakash Chakrabarty and Brinda Sen of Routledge for their e[illegible]uragement, assistance, and patience.

AM

RW

CONTENTS

PREFACE

National security is at the heart of contemporary public policy debate. Not only the conventional domains of intelligence and terrorism, but the economy, scientific research, education, and even the COVID-19 pandemic are in the cross-hairs of national security. In several cases, this extension of the reach of national security makes sense. In others, however, the concept has been used to justify government restrictions of fundamental rights. Two elements whose role in the debate requires closer scrutiny: the positioning of national security in the theory of power, and the controls on the factors that facilitate its application. In other words, is national security a purely political category or should it be accorded legal status? It is also important to understand the extent to which States are able to exert control over the increasing presence of the technology of information in the national security field.

National security does not ineluctably transcend other social, political, and economic goods. Furthermore, it is difficult to weigh competing concepts that belong to different domains; attempting to balance political and legal interests rarely produces a satisfactory outcome, as their respective weights are measured according to different standards. The primary issue, therefore, is to determine whether national security is meant to protect the State or the citizen. If it is the former, individual rights may be sacrificed to protect the State, hence rule by law. If the latter, the protection of the citizen is at the core of national security, hence the rule of law.

This choice is obviously a function of the nature of the State. An authoritarian regime is likely to reach a different balance than a democratic one. But this question is bedevilled and disrupted by the widespread availability of the technology of information. Governments cannot resist the acquisition of 'AI-powered' pre-emptive policing and the promises of 'Big Data-enhanced' decision-making. At the same time, however, the borders have dissolved between military and secret service technologies, on the one hand, and civil society, on the other. Private individuals can easily hide themselves from the prying eyes of government. They can organise groups of activists

and social unrest at the click of a mouse. They can threaten the economic order by creating alternative ways to create and exchange value, and unsettle financial markets. What is rarely taken into account, however, is the role of the (relatively) few companies that control these technologies and run them according to their own business needs rather than in the interests of the public. Defence and law enforcement contractors are not a novelty in the (national) security business. But what has changed is the leeway they now enjoy. A private company—we analyse the cases of Adobe and Venezuela, as well as of Google and Huawei—can paralyse an entire country or disrupt a multinational business merely by revoking a copyright licence. And this may occur as a result of a government order. Nothing, however, prevents a company from deciding unilaterally to interfere in the jurisdiction of government; it happened in the legal battle between Apple and the FBI concerning the cracking of iPhone security to support a continuing investigation.

But there is a subtler and more troubling and concern-raising issue: the direct control that Big Tech is able to exert over billions of human beings by controlling the interfaces of the computer programmes made 'freely' available to people. No matter the place, the culture, the educational level, or the economic circumstances, everybody must behave according to what the interface of a messaging application or a social networking platform tells them to do. And they comply. No government, even the most authoritarian, could dream of achieving this level of conscious and spontaneous compliance.

As much this scenario may resemble the plot of a dystopian novel, it is not simply because it describes reality, but because governments have convinced themselves that they could maintain control over their national security strategy by delegating to Big Tech the design of the operations. This serious miscalculation is among the errors we attempt to illuminate in the pages that follow.

1

THE EVOLUTION OF NATIONAL SECURITY

The dangers of disloyalty and betrayal generate suspicion and distrust. Those who govern societies large and small naturally seek protection against the threats of social turmoil, treason, and public disorder. The means by which these forces may be contained are today encapsulated within the general notion of national security. This chapter traces this development over many centuries, attempting to elucidate the fundamental characteristics of this inevitable feature of social organisation and administration.

The Greek genesis

Being born in Sparta around the beginning of the 9th century BC was a guarantee of an arduous life. From the age of seven, assuming an individual was considered by the council of elders (the γερουσία) to be worthy of being kept alive, a male would be removed from his family to be enrolled in the ἀγωγή, the ruthless education system. Females were prescribed less harsh but severe training that included the physical and mental rigours of gymnastics, poetry, and military exercise.

That was, however, still inadequate. According to the Xenelasian Law passed by King Lycurgus, a true Spartan was forbidden to have contacts with other peoples, but only with the edge of his sword, the ξίφος. The logic behind the Xenelasian Law is well elucidated in Plutarch's account of the Spartan king's life:

> And this was the reason why he forbade them to travel abroad, and go about acquainting themselves with foreign rules of morality, the habits of ill-educated people, and different views of government. Withal he banished from Lacedaemon all strangers who would not give a very good reason for their coming thither; not because he was afraid lest they should inform themselves of and imitate his manner of government (as Thucydides says), or learn anything to their good; but rather lest they should introduce something contrary to good manners. With foreign people, foreign words must

DOI: 10.4324/9780367809775-1

> be admitted; these novelties produce novelties in thought; and on these views and feelings whose discordant character destroys the harmony of the state. He was as careful to save his city from the infection of foreign bad habits, as men usually are to prevent the introduction of a pestilence.[1]

The Xenelasian Law, ultimately one of the causes of the quasi-extinction of the Spartan 'breed,' contributed to the preservation of the system of values that kept Sparta united and strong: untouched and untouchable by the 'infection of foreign bad habits' and the 'novelties in thought.'

Ethical considerations apart, the Lycurgus rule was an early acknowledgement of how important a strong allegiance to an idea was to guarantee an effective and seamless protection of the State from foreign threats and, less intuitively, from internal *coups*.

Athenians were not alone in choosing a different path from the Austinian 'rules backed by sanctions' approach to law[2] that corresponds to the Spartan theory of power:

> Athens also exhibited a high level of social order. Most Athenians appear to have fulfilled their public duties with remarkable regularity … Athens' economic success would not have been possible unless Athenians could normally rely on compliance with the requirements of fair dealing and other business norms in ordinary commercial transactions. And here is the paradox: order was maintained despite relatively weak mechanisms of formal coercion.[3]

A police force, in the sense of a structured, State-controlled law-and-order enforcing organisation, did not exist, and the actual enforcement was delegated to slaves operating under the authority of a magistrate to 'calm' riots and arrest criminals. Statutes had limited deterrent effects because 'Athenians juries did not enforce clearly defined statutory norms in a consistent and predictable manner.'[4] Compliance with the law, while still being a matter of self-restraint in pursuit of self-managed vengeance delegated to the 'State,'[5] relied heavily on socially imposed sanctions[6] rather than being a task solely attributed to law enforcement.

In short, both Sparta and Athens grounded their public (order) policing strategies on a set of core values which were fundamentally different

1 Dryden 1910: 70.
2 Austin 1832. See Wacks 2021a: 79–82.
3 Lanni 2016: 2.
4 Ibid: 3.
5 Herman 2006: 190–191.
6 Hunter 1994.

and enforced in peculiar ways to achieve different certain goals: controlling power by denying openness and independence (Sparta), and delegating the peace of inhabitants to themselves rather than to an omnipotent and omniscient *über* entity (Athens).

Roman roots

The development of Roman rule demonstrates a somewhat peculiar perspective in the management of (what we may call) public order and national security. In contrast to the Spartan approach, Roman culture was never either exclusivist or refractory to foreign ideas—as Horatius' iconic verse, *graecia capta ferum victorem coepit*,[7] brilliantly encapsulates.

This does not mean, of course, that there was no need to 'protect' Rome's values from the infection of 'foreign bad habits' as the life and works of Cato the Elder revealed to historians. In fact the struggle between tradition and external influences occurred in an evolutionary manner. And, pragmatically, it led to a notion of (what now we call) public order and public security/safety that was more functional than structural considering, too, the growing expansion of Roman borders that required a more organised and effective administrative structure.

> Since in the Roman era a police force did not exist as such, and policing was undertaken by different kinds of subjects, it is not correct to talk about a specific police force whose duty was to monitor, prevent and repress socially dangerous activities.[8]

In antiquity punishment was administered by the political ruler 'on behalf' of the divinity's will, and the suppression of 'criminal' activity was inspired by religious creeds rather than by the law. With the coming of monarchy, the situation began to change.

> In the Rome of Kings, the *viatores* and the *lictores* were those who assisted the king in his duty to preserve order in the town and to punish all conduct regarded as reproachable.[9]

During the Republic, the military was forbidden to cross the *Pomerium* (the *Urbs*' boundaries); therefore it could not secure law and order. It was the duty of various magistrates, mainly by way of the enforcement of a set of powers collectively named by scholars '*Coercitio*,' to resolve internal

7 Horatius, *Epistole*, II, 1, 156.
8 Purpura 1985: 101.
9 Ibid: 102.

disputes. But the main focus of the administration was on behaviour that might pose a danger to the establishment: from the settlement of citizen groups not subjected to public control to (real or supposed) conspiracies and heinous crimes such as arson, rape, and homicide. Other offences not considered sufficiently important to be handled by the rulers were left to the 'private' management of individuals.

The ubiquitous, transnational, and eternal 'public morality' was the object of the *Iudicium Censorium* issued by a special magistrate, the *Censor*. In this regard it is interesting to analyse the dynamics of this approach as it represents the connection between the protection of sacred principles—central to the notion of public order—and the quotidian political struggle. Originally, Censors were supposed to handle, among other things, the *census*, i.e. to record names of citizens and their possessions, and place them into 'tribes' which entitled them to vote in an election. The Censors' obligations were not strictly regulated by the law; therefore, for instance, they might decide on their own how many people had to be included in tribe A, and how many in tribe B. Thus, *de facto*, they controlled the expression of political choices of the citizenry.

As a result, the Censors possessed the power to deprive individuals (but mainly those who belonged to the ruling class) of their rank and character through a special trial called *animadversio censoria*.[10] If convicted of violating the *boni mores* (Roman traditions) or the rules of the town, he would be marked by the *ignominia*, a punishment that essentially meant the forfeiture of the franchise or being relegated to a less powerful tribe.

What rendered the Censors so powerful was the fact that the possession of civil rights was, in the Republican era, the main characteristic of *Libertas* (freedom). But freedom was not possible without *Pax* (peace): 'ego omnia ad libertatem, qua sine pax nulla est.'[11] And *Securitas* (security) was the result of the simultaneous interaction between the former two virtues: '*Pax* together with *Libertas* means *Securitas*.'[12]

The Imperial age entirely altered the approach to the management of public order. In contrast to Republican times, the military were authorised to enter into Rome and become an instrument of law enforcement. At the same time, the emperor established his own personal guard that never left his side, even when he appeared in the Senate. In parallel, public order was enhanced by the integration of the social groups that gained some sort of prominence, thus reducing the possibility—and the violence—of protests and public disturbances. But under the Empire, the ties that once united *Pax*, *Securitas*, and *Libertas* began to unravel. Lucius Annaeus Seneca advocated that

10 Adams: 118.
11 Cicero, *Epistulae ad Brutum*, 2, 5, 1.
12 Lana 1990: 57.

> *Securitas publica* is also described as the benefit of peace, a fruitful rest, the free enjoyment of one's time, and a calm that is not disturbed by public preoccupations, which exempts citizens from all their obligations, such as brandishing weapons in defence of the State. It is from such a *securitas* perspective that the philosopher finds *pax* and *libertas* considered as indivisible goods. The *libertas* here is no longer the one, conceived by Cicero, which essentially consisted in the exercise of citizens' rights. Peace is no longer the imposition of Rome's will on all peoples. Peace, that is to say *securitas*, is a good in that it allows us to live in safety from dangers.[13]

In reality, however, *Pax Romana* or *Pax Augustea*[14] was built upon a power that permitted all (conquered) States to live in peace and harmony under Roman rule.

The Republican ideal of life as a combination of peace, freedom, and security simply failed, and Imperial peace, as Tacitus brilliantly puts it, granted *tranquillitas, non libertas* (peace, not freedom.)

The core of the newfound *tranquillitas* of the 'restored' Republic, as the emperor used to call his absolute rule, was Augustus' legion-based military system whose deployment was not confined to the waging of 'conventional' warfare:

> Augustus and his successors during the first century of the Empire did not rely on any one agency in particular to detect and to expose subversion. They used informers – *delatores* – to reveal a wide range of crimes, real and imagined. In addition to informers, the first emperors efficiently used the praetorian guard, especially its centurions and tribunes, to act as plain clothes men to arrest those accused of treason.[15]

But it was not long before the increasing need for information-gathering led Augustus' successors to enhance the use of 'unconventional' methods to secure the survival of the Empire:

> Emperors continued using different types of soldiers for occasional missions, but a new military institution of the later principate

13 Hasic 2016.

14 So named after the emperor, Gaius Iulius Caesar Octavianus Augustus, whose political achievements lasted for about 200 years, from 27 BC to 180 AD.

15 Sinnigen 1961: 67.

> started performing many of these special policing tasks, such as execution, arrest and domestic espionage: the *frumentarii*.[16]

The *frumentarii* was a corps of soldiers tasked to collect wheat (*frumentum*) and taxes from the provinces of the Empire; to accomplish this they needed to possess special qualities:

> They were very skilful, cunning and intelligent because, through information, they knew where to find wheat and other grains to store and distribute to their legion. Through this research, they were able to know, discover, see, hear and move in 'enemy' territory and all the information could be useful. They were probably also controllers and responsible for the grain warehouses that were built in the frontier lands.[17]

The ruling of Emperor Domitian (81–96 AD) was the first to expand the *frumentarii*'s duties to support the harsh suppression of the Stoics and other sceptical scholars whose ideas were considered to threaten the Empire. The repression was not limited to (literally) burning books promoting their 'subversive' messages, but was enforced against those who supported their philosophical works:

> *Triumvirii* were ordered to burn … the ingenious writings of those clever intellectuals. The flames were supposed to silence the voices of the Roman people, the freedom of the Senate, the conscience of the human race … Just as we once clearly defined the idea of freedom, so today we celebrate slavery, since delusions and inquisitions prevent us from speaking and listening. And together with our voices we would have lost our memory too, if we could forget as easily as we stay silent.[18]

But it was Emperor Hadrian (117–138 AD) who turned Augustus' *frumentarii* into executioners and spies.

> The first documented evidence of *frumentarii* as detectives actually comes late, in the reign of Hadrian, who had them informing on his friends in the imperial court. The wife of one of them frequently wrote to her husband complaining that he spent too much time in the city enjoying himself and never came home to her. Hadrian found

16 Furhrmann 2014: 152.
17 Guerra 2010.
18 Tacitus, *Agricola*, 2. English translation by Andrea Monti.

> this out through his spies (*per frumentarios*) … Their secret service duties, besides investigation and arrest, eventually included political assassination. *Frumentarii* were so employed under Commodus and Didius Julianus.[19]

Over time, the power of the *frumentarii* developed to a level where the powers-that-be could no longer ignore the protests and concerns raised by the 'free hand' they had been given and by the methods they practised to enforce the orders emanating from the Empire:

> In their pursuit of political criminals they penetrated the cities and villages, searched private homes, and exacted bribes. This was especially true in connection with the frequent military expeditions of the emperor.[20]

As untenable as the *frumentarii* methods had become, no ruler could restrain himself from collecting information to protect his reign. This explains why the Emperor Diocletian (284–305 AD) dismantled the despised *frumentarii*, but at the same time created a new, and more feared, entity: the *agentes in rebus*.

Diocletian was deeply aware of the necessity of an efficient system of information-gathering not only to deal with domestic security, but also to plan political and military actions. It was not a surprise, therefore, that an important part of his broad reform activity was dedicated to the design of this new service. In contrast to the *frumentarii*'s status, the *agentes* were firmly incorporated into an administrative structure that even included a training facility, the *schola agentum in rebus* under the authority of the *Magister Officiorum*, and at the end of their service they were moved to other sectors of the administration.

To be admitted to the *agentes in rebus* corps, a candidate had to be a free man, have a 'clean record,' and his origin and previous assignments were scrutinised to be sure that he was not *indignus*. A law passed in 382 AD under the ruling of Valentinian II specified that even the emperor himself could not interfere with the selection process to guarantee the rectitude and probity of those enlisted. This may well have been a smokescreen as the methods enforced by *agentes in rebus* were similar, if not identical, to their loathed predecessors.[21]

The assimilation of these Roman entities into modern secret services was pointed out by Sinnigen, and, more recently, by Sheldon. Notwithstanding

19 Sheldon 2004: 253.
20 Ibid: 257.
21 See Guerra 2011.

the broad reception of this apparently persuasive thesis, it has been criticised on the ground that the actual role of the *agentes*[22] was limited; they had little influence over the course of political events. *Fumentarii*, *agentes*, and *curiosi* have played an important role in the architecture of Imperial security, though without assuming the status of military police or law enforcement.[23] As will become clear below, indeed, a genuine actual police apparatus would not appear before the arrival of Napoleon Bonaparte, while in Rome and in *Nova Roma*, public order and public security (to use these modern concepts) have been characterised by specific goals or objectives rather than by the establishment of administrative apparatuses explicitly dedicated to this end.

Even in their limited extra-duty activities, though, the *agentes* were an important component of the Empire (or emperor's) system, further enhanced by the creation of the *cursus publicus*. Created by Emperor Augustus in about 20 BC, while the 'Imperial Postal Service' does not wholly account for the true nature and importance of the *cursus publicus* for the protection of the Empire, it was a complex infrastructure of land, sea, and fluvial roads, as well as of staging posts and transportation means, where the messengers could travel thanks to the provision of well-fed and properly rested horses and other efficient and effective means by which to deliver their messages, but at different speeds, according to the urgency of the information they were carrying.

When the emperor began thinking about the *cursus publicus* he had several possible sources of inspiration since he must have been aware of the Persian, Egyptian, and Caesar's antecedents, yet:

> [W]e should not rule out the possibility, however, that the idea for a service originated with Augustus's own observations and imagination. He had far too much political insight not to see that the fall of the Republican government was partially due to the absence of an effective central administration, causing an inadequacy of coordinated action, a lack of consistency of policy, and an inability to control ambitious provincial magistrates. To accomplish all these goals himself, Augustus would need a centrally administered communications system, in order to ensure his own security and to buttress the stability of the empire.[24]

22 Purpura 1973: 165–273.

23 For a critical analysis of the role of the *Agentes in rebus*, dismissing the theory that they were a 'secret police,' see Purpura 1979.

24 Sheldon 2004: 144.

These two components were closely connected. If the *agentes in rebus* were the 'muscles' of the Imperial messaging and, occasionally, intelligence system, the *cursus publicus* was a sort of an *ante litteram* Internet: an infrastructure allowing the *agentes* to transfer information rapidly and efficiently. Moreover, under the rule of Emperor Constantius II (337–361 AD), the exercise of surveillance was delegated, to a selected group of *agentes* called *curiosi*.

The use of *cursus publicus* was initially reserved for the emperor's issued or addressed communications, but over the course of time the passage of military supplies, and access to the service by dignitaries and religious authorities[25] were allowed, thus turning it into a rather voracious resources-eater, leading to its drastic restructure.

Before its final demise, however, *cursus publicus* maintained its key role in the Imperial security infrastructure. In fact, the Byzantium Empire, established in 395 AD from the ashes of the old Roman Empire, still managed its security by way of the *cursus publicus* (whose control was latterly assigned to the λογοθέτης τοῦ δρόμου) and expanded the operation of the *agentes in rebus* and the *curiosi*.

Confronting a different (geo)political and economic situation, though, *Nova Roma* rulers were soon to develop a different approach to the security of the Empire:

> Renewed by Constantine the Great at the beginning of the fourth century and surviving until 1453, [the Empire] was a complex, multi-ethnic state, almost constantly under attack, always forced to spend most of its resources to survive. Many citizens … were closer in language, culture, religion … to more or less barbaric – and often hostile – peoples stationed outside the borders … than the Greek-speaking ruling classes of Constantinople.[26]

Furthermore, borders tended to change frequently, leaving the inhabitants one day subjects of the might of Empire, and the next day subjects of a neighbouring sovereign power. They might then revert to Byzantine rule! That perpetual political instability, which made it difficult to distinguish friend from foe, placed the Empire in a very different position from the mighty Republican and Imperial Rome, thus requiring a new strategy for managing security.

Republican and Imperial Rome both boasted a formidable apparatus that used its strength as a military deterrent, in a condition of superiority against most of its enemies, generally deploying spies for domestic security rather

25 Breccia 2019: 51.
26 Ibid: 7.

than in foreign politics and war.[27] *Nova Roma*, in contrast, was in 'survival mode': other than having to prevent internal coups (over 11 centuries only 8 Byzantium emperors did not die of natural causes) it was constantly under attack from external threats, and this explains the adoption of a broader approach to the security of the Empire.

The 'traditional' information-gathering about enemies and (temporary or unreliable) friends was converted into what we would today call a 'strategic analysis':

> [A]dapting to enemies will become a guiding principle of the military art of Nova Roma … learn how to prevent threats, but also to exploit the weaknesses of different enemies by changing its own behaviour opportunely.[28]

In other words, the 'scale' of intelligence activity progressed from a tactical/operative level (obtaining information relevant to a specific task such as enemy locations or formulating a plan to counter) to a political/strategical one (defining the political goal and the strategy to achieve it). Eventually this strategy was integrated into a system of cultural and religious assimilation of the members of—not yet or not very—hostile countries by supporting the spread of Christianity and, more prosaically, hosting at the emperor's court members of the neighbours' élite class that, in reality, were hostages rather than guests!

This forced permanence at the emperor's court was not merely a means by which to ensure that his neighbours did not attack the Empire. During their stay in this golden cage, but not always with positive outcome for the Empire,[29] the 'guests' were exposed to (or brainwashed into accepting) the religious and cultural foundations of Byzantine values, in particular, the special role of the emperor. In contrast to other traditions, where the sovereign was a god himself (Egypt, Japan) or was turned into a god and venerated as such (Rome), the choice to submit the Empire to Christianity turned the rulers of Byzantium rulers into 'simple' men, albeit men blessed with a deep connection to the divine laws.

As a consequence, there was no blood-based 'inheritance' of the throne: the successor was designated by the ruling sovereign, and it was up to God to allow him to live long enough to claim his position.

27 Preto 1994: 18–19.

28 Breccia: 19.

29 In 461 AD Teodoric, later Teodoric the Great, King of the Ostrogoths, was taken hostage by Emperor Leo the Thracian as a guarantee of compliance to a treaty signed between the Byzantine Empire and the Ostrogoths. He was freed after ten years of detention and Imperial 'cultural education' in Constantinople. Teodoric had no qualms about marching against his former captors.

The practical outcome, with respect to legitimacy, was that 'everybody' could seize the power by violent means (*usurpatio*) and obtain, as a matter of fact, a God-given right to absolute power. On the one hand, it is therefore evident that the emperor-in-charge was surrounded by an impressive security apparatus, and that obtaining in advance information about possible coups was a major priority. On the other hand, however,

> [I]f the *Basileus* is dear to God, it is God who will remove the threat from his head. A successful *coup* could be interpreted as the manifestation of providence, which punished an unworthy ruler by allowing his elimination. The success of a conspiracy led to prudence in judgment, since, in his inscrutable omniscience, the Lord had turned his eyes away from the victim: it was a very fine line between a criminal act and an instrument of supreme justice.[30]

As opposed to the past, and to the near future of Western monarchies, 'emperor' was synonymous with 'Empire'; therefore when it came to domestic security the allegiance to the emperor was not always clear or unquestionable.

> Defending the capital, therefore, involved a constant balancing act between financial, political and logistical factors. And in the light of these, it seems not surprising that no permanent military force of any size was ever stationed permanently within the city walls. Those units which were in Constantinople were kept, to a degree at least, under separate chains of command, to minimise the possibility of their uniting against the emperor of the day.[31]

It is therefore safe to conclude that there was no material distinction, in regard to strategy, between domestic security (as a synonym of the emperor's protection) and border protection (as a synonym of the Empire's defence.)

The essence of the new Byzantine approach to total security and defence is represented by the *Strategikon*, a long-lost treatise on the art of war, attributed to Emperor Maurikios (582–602 AD), only recently rediscovered; it is one of the classics of ancient warfare.[32]

30 Breccia: 33.

31 Haldon 1995.

32 'The text of the *Strategikon* was not published until 1664, at the back of the antiquarian and decorative *Techne Taktike* of Arrianus, a Roman officer, albeit writing in Greek, and therefore the more prestigious. Even after 1664, neglect long persisted, for with the Enlightenment came the black legend of Byzantine minds paralyzed by obscurantist religiosity, and so it was that the *Strategikon* was not rediscovered until the eve of the twentieth century,

> Warfare is like hunting. Wild animals are taken by scouting, by nets, by lying in wait, by stalking, by circling around, and by other such stratagems rather than by sheer force. In waging war we should proceed in the same way, whether the enemy be many or few. To try to simply overpower the enemy in the open, hand in hand and face to face, even though you may appear to win, is an enterprise which is very risky and can result in serious harm. Apart from extreme emergency, it is ridiculous to try to gain a victory which is so costly and brings only empty glory.[33]

Power on the battlefield has changed. The Eastern Roman Empire is no longer the feared and invincible war machine of the past. Too few are the enlisted; too wide the borders to defend. This is why the *Strategikon*:

> conceives a useful war, based on the useful and unscrupulous use of every possible expedient … there is no hint of the possible respect of rules, no hesitation in using any available means against the enemy because war is a disease that must be limited and solved quickly and painlessly, all the better if you avoid the direct use of military force, always expensive and full of risks.[34]

This reality check is what Edward Luttwak calls a brilliant 'grand strategy' by which one

> turn[s] the very multiplicity of enemies to advantage, by employing diplomacy, deception, payoffs, and religious conversion to induce them to fight one another instead of fighting the empire. Only their firm self-image as the only defenders of the only true faith preserved their moral equilibrium. In the Byzantine scheme of things, military strength was subordinated to diplomacy instead of the other way around, and used mostly to contain, punish, or intimidate rather than to attack or defend in full force.[35]

Using religion as a key part of the Imperial security strategy nevertheless had its drawbacks. As mentioned above, converting (or attempting to convert) a non-Christian population to the Holy Spell was one of the methods by which to secure the allegiance of those who posed a threat, if not to the

---

eventually attracting the interest of strategic theorists and even practitioners, who could best recognize the real expertise it contains,' Luttwak 2009: 266–267.

33 Dennis 2001: 65.

34 Breccia: 79.

35 Luttwak: 409.

'Vice-regent of God,' as the emperor has been called,[36] at least to its creed. Furthermore, as discussed above, both the human *substantia* of the emperor, and the fact that he derived his power from a complete and unquestioned acceptance of the divine law were fundamental to his authority. Yet it must be acknowledged that he had, at least in theory, to submit to the religious authority, the patriarch.

The inescapable result was that to use religion as a part of his global security strategy, the emperor had to accept a significant limitation of his powers. This he could not accept with equanimity, and, with varying degrees of success, emperors sought to impose their will on the patriarchs. A political contest was disguised as a theological argument.

European advances

The political fragmentation of the following centuries did not alter the 'national security' debate, except perhaps in one aspect: the loss of centrality of the *boni mores* or its equivalent as the foundation of the control and surveillance of the citizen. It is true that religious differences continued to support contesting political goals which resulted in long and bloody wars. Nonetheless, at least initially, during the various major and minor reigns in Europe as well as during the Middle Ages in Italy, the question of 'national security' was treated for what it was—the protection of the rulers.

> Security and defence, also perceived as fundamental common goods by the city society – ready to organize itself in spontaneous formations to guarantee internal order and also ready to submit to military recruitment periods to protect the city from the external threat –, become the exclusive prerogative of political power and its organs: instruments and public, rather than collective, values. The passage from the *bonum commune* to the *bonum publicum* marks, also in this relevant sector of the city life, a gap between two different forms of order: one including social plurality, the other monopolizing and only abstractly representative. If, in fact, on the one hand, the public assumption of security and defence instruments obviated the precariousness and inefficiency of an autonomous social organization, on the other hand, it was in fact worth putting the military and police forces at the service of the hegemony of the 'party' in power.[37]

36 Geanakoplos, Deno 1965: 386.
37 Treggiari 2011: 266.

It is a safe assumption, though, that ruling élites neither owned nor cared about an abstract idea of 'public order' as a synthesis of the social principles that constituted the core of a society.

> Early Middle-Age legal system ignored the notion of 'public order' and there was no connection with a public ruling. Characterized by a juridical ideology that intertwined and confused public and private in the field of criminal repression, those systems barely felt the control of violence as a public prerogative, limiting themselves to the mediation of political power against the inveterate practice of private self-protection through the remedy of the patrimonialization of offense, in an attempt to direct society towards peace. It was, however, always the initiatives of the private sector, in those societies, which absorbed almost all the activities of vigilance and prevention. It was always the private individuals who had to work to identify, capture and bring to justice the perpetrators of the transgressions from which those same individuals had been harmed.[38]

Since 643 AD with the *Edictum Rotharis Regis*, and even earlier, the legal system of the Longobards distinguished between offences against the sovereign power, on the one hand, and private disputes between individuals, on the other. The former, such as high treason or conspiracy, were dealt with directly by the authorities and attracted the death penalty, or if the 'trial' was conducted *in absentia*, with the *bannum*. 'Private crimes' such as killing a free man were no longer punished with the old institution of *faida* (the collateral vendetta, to be waged against the relatives of an assassin), but with the payment of a certain sum of money, the *widrigild* (weregild).

The main explanation of the non-involvement of the sovereign power in the affairs of citizens—and thus the lack of a properly established security and police apparatus—was the principle that governed criminal trials: the absence of a presumption of innocence..

> This distribution of procedural positions presupposed a conception of evidence as a means of exoneration and was consistent with the structure of the early medieval judicial procedure (essentially identical in civil and criminal cases), in which the judge, who represented the *publicum*, since he did not have an interest of his own, did not enter into the merits of the case, limiting his role to activating the procedure and checking the regularity and outcome of the evidence on which the parties tried their case.[39]

38 Ibid.
39 Treggiari: 267.

Around the middle of the 13th century the rise of city-states saw a growing interest in the active involvement of the central powers in citizens' (criminal) behaviour.

Petty crimes were still dealt with in the previous way: combat between the parties with the system providing only enforcement of the outcome. Major offences, in contrast, were directly investigated, prosecuted, and tried by the justice system. The rulers' motive for this intrusion into the trial of conduct that threatened order and morality was

> the need to affirm the pre-eminence of the *Comune* over the citizen … The crux of the matter is all in this hairpin bend which, as we know, has a very strong political motivation, made up of concern for the effectiveness of the law and the credibility of political power, concern for *concordia civium* and fears for public order. It is no coincidence that this is one of those issues that were decided by practice, driven by practical needs and political necessity, and only later was it, so to speak, rationalized by doctrine.[40]

The outcome was the establishment of

> a specialized surveillance, repression and security bodies – the police, therefore, as an institution linked to the municipal offices that administered justice – and (military activity being an aspect of civic discipline) the formation of a municipal militia to be employed in external military activities, to meet the needs of defence and war.[41]

The notions of public security, public order, and State security were, of course, not well defined or differentiated as legal categories, overwhelmed as they were by the political struggles and the wars fought between the 13th and 14th centuries that led to the demise of the *Comune* and the rise of the *Signorie*.

A distinctive feature of the *Signorie* era's approach to public order and security, apart from the extensive use of spies and informers, was the institutionalisation of the direct involvement of the citizen in the threats or the crime-related information-gathering process. As discussed above, since the Roman period, *delatores* and various types of informers were widely known and used, but what transpired in Venice was rather special:

40 Sbriccoli 1998: 231–268.
41 Treggiari: 270.

> [I]ntelligence services and especially counter-espionage … need the effective collaboration of the state apparatus and citizens, convinced of their moral and civil duty to contribute to common security … Since 1400 Venice has been devising a refined method to stimulate the cooperation of its citizen … in the collection of information and secrets relating to economy, public administration, state security.[42]

Recognising that information is a good and that every good has a price, Venetian authorities formalised the activity by creating the *Raccordo*, known also as *Ricordo* (remembering) or *Secreto* (secret). The *Raccordo* was a sort of affidavit that allowed every citizen to notify the authorities of (alleged) important information about the ruler's security, expecting in exchange the acknowledgement of their *Supplica* (an application for a licence, monetary support, a job, and so on):

> [T]here is no sector of public life in Venice that escapes the attention of the *raccordanti*: bandits, blasphemers, thieves, pimps, sodomites, seducers of workers, concealment of corpses, illegal possession or export of weapons, escapes of convicts, escaping from prisons, but also projects for new prisons, gangs of pickpockets and robbers, smugglers … tax evasion … violations of health laws, falsification of public and private scripts, possession of heretical books or manuscripts, abuse in office acts … machines and military secrets.[43]

This far from exhaustive list accounts for the security needs that arise from the growth in complexity of society. Long gone are the times when the most important use of an informer was to dismantle an act of treason or to know in advance the location of enemy troops.

The *Raccordi* were not, however, the only weapon available to the Venetian authorities. The demand for iron-clad control and repression of political dissent was fostered by an extensive use of spies and informers at the service of the 'public prosecutors': the much-feared *Inquisitores*.

> The control and increasingly attentive repression of political, religious and social dissent by the *Inquistores* can be seen in many measures, from the *Prigione dei piombi* with the annexed *Camera del tormento* made available to them, to the improvement of the system of *Boche del leon*[44] and secret denunciations, to the sanctions

42 Preto 1994: 154.
43 Ibid: 159–160.
44 The *boche de leon* (lion's mouth) were lion-shaped masks made of stone located on the balcony of Palazzo della Signoria in Venice that resembled post boxes. By leaving an anony-

> against novelists and rapporteurs … [that] … indicate a desire for global control of citizens' thinking.[45]

In parallel, the *Consiglio dei dieci* (Counsel of Ten) was established in 1310 as a temporary special prosecution service to hunt down the Tiepolo conspiracy, but was then converted into a permanent institution of the Republic of Venice, extending its reach from the control of political dissent to public order issues such as prostitution, gambling, and the control of foreigners.

Venice was, of course, by no means the only State to keep its citizenry on a short leash, as the other sovereign powers ruling Italy and Europe were equally interested in maintaining a strong grip over their people. But none established an actual and effective public security apparatus until Napoleon Bonaparte.

Initially, France, although not yet an actual empire, pursued the path paved by the Roman Republic. Thus in 1032 the Capetian King of Francs, Henri I, stripped policing duties from the Vice-count of Paris (a member of the royal establishment) and passed it to a magistrate, the *Prévôté de Paris*. This did not, however, improve matters, as 'Paris will remain, in the following centuries, the capital of insecurity, preferred den for depravities and infamies.'[46]

A similar destiny was reserved for the attempts that followed to find alternative solutions; for centuries to come, the French approach to public order and public safety/security proved to be fairly ineffective. In 1254 the need to keep towns safe at night led to the creation of the *Chevalier du Guet*. In 1306 a further office of magistrate was established, the *Commissaire examinateur au Châtelet*, who was given both policing and judicial powers. And in 1526 a typical public security issue, the policing of begging, homelessness, and other similar social problems, fell under the jurisdiction of a lower magistrate, the *Lieutenant criminel*, who had judicial powers.

It was only towards the end of the 17th century that a more structured approach towards public order emerged, thanks to an edict proposed to King Louis XIV by his powerful minister, Jean-Baptiste Colbert. In 1667 Colbert, witnessing the failure of French security, understood the need to address the issue with a structured approach that was included in the *Édict* that created the *Lieutenant de police*:

---

mous letter in the lion's mouth, every citizen could report (alleged) wrongdoing to the magistrates.

45 Preto: 186–187.

46 Cancès 2019: 42.

> Policing means safeguarding public peace and, in particular, protecting the town from causes of disorder, providing prosperity and ensuring that all live according to their condition and duty.[47]

This office lasted until the French Revolution in 1789, and was so successful that it was extended to other large cities.[48] But the quantum leap in establishing a serious management of the policing-by-police approach came with the rise to power of Napoleon Bonaparte and the creation on 17 February 1800 of the *Préfect de police*: a comprehensive re-thinking of the public security apparatus.

The influence of Bonaparte on the management of public security goes well beyond his short-lived empire: his 'successor,' King Louis XVIII, after having endeavoured to dismantle Bonaparte's public security machine, quickly changed his mind and re-enacted it as quickly as he could because of its political usefulness in protecting it, and political power in general, from the revolution.[49]

In this respect it is interesting that the modern French 'public order' is defined as

> the collection of conditions—legislative, departmental, and judicial—which assure, by the normal and regular functioning of the national institutions, the state of affairs necessary to the life, to the progress and to the prosperity of the country and of its inhabitants.[50]

The word order of this provision is revealing. According to Bernard Burke's *The Book of Precedence*,[51] the sequence of words sets the priorities. In this enactment, first come national institutions, then what is necessary for the survival of the country, and, last and least, the inhabitants.

But the influence of Bonaparte was not, of course, limited to France, as most other European nations still base their legal and administrative systems on this approach. So, for example, the contemporary evolution of German law is well within a democratic approach to public order, but this did not prevent German scholars of the early 20th century from adapting

47 'La police consiste à assurer le repos du public et des particuliers, à protéger la ville de ce qui peut causer des désordres, à procurer l'abondance et à faire vivre chacun selon sa condition et son devoir quoted from Édit de création de l'office de Lieutenant de Police de Paris (15 mars 1667),' *Musée Criminocorpus*, https://criminocorpus.org/fr/ref/25/17096/ (visited 27 August 2019). Translation by Andrea Monti.

48 Poisson, Philippe *15 mars 1667: Création de l'office de Lieutenant de Police de Paris*, https ://criminocorpus.hypotheses.org/17397 (visited 27August 2019).

49 Cancès: 49.

50 Bernier 1929: 84.

51 Burke 1881.

Napoleonic ideas to the *zeitgeist*. The Prussian Empire's doctrine advocated that its government

> does not seek primarily the comfort and happiness of the individual but rather the power and greatness of the State, since without the latter general prosperity cannot be secure … It opposes a transformation that would place the government in the hands of changing majorities and subject the army to corrupt parliamentary influences – a statement true not only of Prussia but of entire Germany.[52]

and the 'pan-Germanism' of this approach is confirmed by Ernst Troelstch, who affirmed that his fellow intellectuals 'opposed the democratic fiction that the State is an institution created by the individuals for their own security and happiness.'[53]

As mentioned, the reform of the German legal system after World War II did not discard the French influence, as is clear from the terms used in the police codes ('*Ordnungs- und Polizeirecht*') in all German states. At the constitutional level, though, Germany did not include either a '*sureté*' or '*ordre public*' section. Not surprisingly, though, between 1958 and 1963 the Ministry of the Interior tried to push (to no avail) legislative reform that put under the executive power the management of emergencies of various nature. However, as a remnant from the Cold War, there is a section on emergency powers known as the 'Emergency Constitution' which consists mainly of the *Notstandsgesetze* (Emergency Acts) passed by the Bundestag on 30 May 1968 as an addition to the Constitution, which regulate the state of emergency, or in case of defence from foreign aggression, domestic disorder, or natural disasters.

According to the German regulation, a state of emergency can come into force if an external threat impedes the normal democratic decision-making process, e.g. if the Bundestag or Bundesrat can no longer meet. In this case, a Joint Committee comprising members of the former assumes essential parliamentary functions, but without the power to amend the Constitution. The passing of the emergency laws was, however, preceded by fierce domestic political debate which also contributed to the establishment of the 'Extra-Parliamentary Opposition' (APO).

The critics of the emergency laws referred to the catastrophic effects of the emergency ordinances of the Weimar Republic (Article 48[1]), which conferred far-reaching powers on the President of the Reich in the event of an undefined emergency.[54] It is interesting to note that the Emergency

52 English translation by Willoughby 1918: 273.
53 Troeltsch 1915: 52.
54 Spies, Axel, *rechtsanwalt*, interview with Andrea Monti, 27 August 2019.

Constitution includes regulations concerning the suspension of individual rights.[55]

Although French influence spread across Europe it did not reach Britain until the 18th to 19th centuries with the 1785 (aborted) Pitt's Police Act and the Metropolitan Police Act of 1829. Meanwhile the idea of public order was intended to balance the competing demands of freedom of speech and assembly on the one hand and the preservation of the Queen's peace on the other.[56] And 'peace' is the keyword here to understand the evolution of public order and public security in England and the UK.

Since no Crown-appointed police force was established, the protection of public security was left to citizens who, in various ways, were authorised, or more often compelled, to deal with offenders. The frankpledge system, introduced at the beginning of the 12th century, was a shared-liability rule according to which the leader of a group of inhabitants who was called a tithingman was in charge of a tithing (a legal, administrative, or territorial unit.) He was responsible for ensuring that any individual member of the tithing who was charged with a misdemeanour was presented to the court.

Under the Assize of Arms rule of the 12th century every male between the ages of 15 and 60 was required to keep weapons stored in his house and use them to 'preserve the peace.' Imposed in 1285 by the Statute of Winchester, the 'hue and cry' forced whoever witnessed a crime to summon whoever was available by shouts and cries to apprehend the alleged criminal. Moreover, the statute empowered the Sheriff (whose name comes from the old 'shire-reeve' role of the 11th century) to assemble citizens into a posse and pursue thieves and other miscreants observed in the neighbourhood.

In 1361 the Justice of Peace Act concentrated the judicial and public security powers in the hands of a single magistrate. From the 16th century the Sheriff's role was taken over by a representative of the Crown, the Lord Lieutenant, who 'became the head of each county and the permanent local representative of the Crown. He was responsible for the preservation of public order in his county and was the *ex-officio* commander of its militia.'[57]

The Lord Lieutenant resembles to some extent the Roman *praefectus urbi*,[58] and the fact that, as a direct emanation of the Crown, he was given control over an armed force speaks volumes about the management choices in this matter. It is evident that these early statutes were designed to benefit

55 When emergency laws are in force, constitutional guarantees such as the confidentiality of correspondence and telecommunications and freedom of movement are restricted. A Joint Committee is empowered to issue emergency legislation and declare military service compulsory.

56 Williams 1967: 9.

57 Babington 2015: 179.

58 The *Preafectus Urbi* was a lieutenant of the king that was responsible, with a militia under his command, for protecting public order and keeping Rome safe.

the king rather than the citizenry. They do, in fact, spring from the same rationale: spare the king the annoyance of dealing with his subjects and, at the same time, make the subjects protect him at no cost. Or, to consider the question from a different perspective, as was common in the early Middle Ages, a sovereign cared little about the welfare of his subjects, unless they presented a direct threat to him. In addition, he did not need to maintain a costly permanent police force that might become an alternative, autonomous source of power threatening his own authority.

Thus, while the mandatory enlisting of citizens to provide security 'services' to the community was no longer active, the *private* management of security began to gain momentum. The constabulary/justice of peace policing system was complemented by individuals or groups hired by merchants, traders, and wealthy individuals to provide *ad hoc* security. And those citizens who were unable to recover stolen property or find the thief began to offer rewards to those who would do it on their behalf.

This system lasted almost unchanged until the second half of the 18th century when the writings of Sir John Fielding, the renowned police magistrate, ignited a debate about the need for a central(ly managed) and professional(ised) police force based on the French experience, and robust regulation of the poor, attainable with a synergic interaction between criminal law, administrative regulation, and philanthropy.[59] It took about half a century, however, to embed (some of) Fielding's ideas into law: the Metropolitan Police Act of 1829.

This reform would not have been possible without an important political decision made by the Prime Minister of the day, Lord Rockingham, in 1782:

> Instead of appointing Secretaries of State for the Northern and Southern Departments, Rockingham decided to have in his cabinet one Secretary of State … to be in charge of home and colonial affairs … to be responsible for the preservation of public order in Britain, and in furtherance of this duty he took over a number of important powers which had formerly been entrusted to the Secretary at War, including the control of all the military units within the realm. This innovation brought about a significant shift of responsibility with regard to the employment of troops in civil disturbances. The Secretary at War … had been directly responsible to the king, in his royal capacity as Captain-General of the army. The Home Secretary, on the other hand, was a Cabinet Minister and as such would be accountable for his executive acts to the Government and to Parliament.[60]

59 Wall 2019: 17.
60 Babington: 743–751.

His political motive was clear: put public order control under the *government* and not, as before, under the king, the Commander-in-Chief of the armed forces.

In 1785 London was devastated by public disorder fuelled by Lord George Gordon who, backed by a 60,000-strong Protestant mob, sought to persuade Parliament to repeal the Catholic Relief Act of 1778. After days of unrelenting riots, and the inability of the civil magistrates to restore order, the king ordered the military to crush the protests. But the bloody battle and the king's decision to involve the troops led to recognition that reform of the method of riot control was urgently required:

> The first major policy initiative for a full-time police organisation began in the aftermath of the Gordon riots of 1785 when Pitt introduced his Police Bill. Important here is the fact that the Bill was primarily driven by concerns about disorder rather than crime. The Bill failed to gain assent because of considerable opposition arising through fear of the police developing into a repressive system of policing similar to that operating in France after the revolution of 1789.[61]

Finally, as pointed out above, in a more extensive reform of the system of the criminal justice system, the Metropolitan Police Act of 1829 created a professional police force tasked with law enforcement and public order preservation duties under the control of the magistrates.

Interestingly, the rest of the kingdom did not immediately follow London's lead, and no less intriguingly, the reform of the police force continued to focus on the protection of 'order' rather than the safety of citizens. The political response to this incongruity came about a century later with the passage of the Public Order Act of 1936 to control the activities of British fascists, although it has more recently been enforced against other extremist groups including the IRA.

The Public Order Act was amended in 1986 to render it more suited to contemporary policing. The Act's long title reveals the meaning of 'public order' in the UK today:

> An Act to abolish the common law offences of riot, rout, unlawful assembly and affray and certain statutory offences relating to public order; to create new offences relating to public order; to control public processions and assemblies; to control the stirring up of racial hatred; to provide for the exclusion of certain offenders from sporting events; to create a new offence relating to the contamination

61 Wall: 18.

> of or interference with goods; to confer power to direct certain trespassers to leave land; to amend section 7 of the Conspiracy, and Protection of Property Act 1875, section 1 of the Prevention of Crime Act 1953, Part V of the Criminal Justice (Scotland) Act 1980 and the Sporting Events (Control of Alcohol etc.) Act 1985; to repeal certain obsolete or unnecessary enactments; and for connected purposes.[62]

Again, as in the case of the French definition of public order, the sequence of words suggests the law's priorities. It is plain that lawmakers were chiefly concerned about maintaining public order rather than fostering 'peace' between citizens. The fundamental dilemma of the modern British notion of public order is well explained by Channing:

> Notions which identify the state's obligation to preserve public order are necessarily associated with the protection or the suppression of civil liberties and human rights. Yet whose liberty should be protected? The concept of liberty in the late eighteenth century was appropriated by both the establishment and the radical alike … Nevertheless, decisive definitions of liberty itself are obscured by subjective philosophies and values … This inherent ambiguity in notions of late eighteenth century and early nineteenth century liberty was interpreted by Thompson to mean freedom from foreign domination, absolutism and arbitrary searches of one's home and arrest. It also included equality before the law and the limited liberties of thought, speech and conscience. Within this 'top-down' hierarchy of liberties was a structure which was directed to preserve the power of the state. From this perspective, freedoms such as speech and thought were necessarily limited in order to manage and suppress radical thinkers and militants who threatened the stability of the Constitution. Yet to the political activist or public protester, absolute freedom of speech was fundamental to their philosophy of liberty. Without it there could be no challenge to state autocracy.[63]

At first blush the Public Order Act 1936 might be considered to be the outcome of a specific cultural and political *zeitgeist* peculiar to the UK. Strange as it may seem, however, it echoes the approach of the Italian Fascist Royal

62 Public Order Act of 1986 available at http://www.legislation.gov.uk/ukpga/1986/64/contents (visited 28 August 2019).

63 Channing 2015: 8–9.

Decree of 14 January 1923 n. 31[64] passed to crush political opponents, i.e. anti-fascist groups. This decree is carefully analysed in Chapter 2, where the difference between national security and public order is examined. For present purposes, what is important is the empirical finding that the 'means' to enforce a public order policy are not inexorably connected to an allegiance to any particular political, ethical, or religious beliefs, as the recent disturbances in Spain and Hong Kong clearly testify.[65]

National security and Asian values

Some 5,000 miles east of Rome and 250 years after Lycurgus' anti-foreigners law, the *ante litteram* Chinese social scientist, Confucius, grounded his theory of power on a similar approach to his Western counterparts. As was the case with Roman Republic and Spartan ideas, Confucius based his teachings on the importance of State values in policing citizens' behaviour. In contrast to the Western approach (and to that one pursued by his arch-rivals, the Legalists), Confucius affirmed the superiority of moral compliance with the values of the State over the power of 'mere' legislation as a way to achieve 'harmony' with 'heaven'—the supreme ruler:

1. If the people be led by laws, and uniformity sought to be given them by punishments, they will try to avoid the punishment, but have no sense of shame.
2. If they be led by virtue, and uniformity sought to be given them by the rules of propriety, they will have the sense of shame, and moreover will become good.[66]

In an apparently stark contrast to the Spartan approach, Confucianism seems 'peaceful' (respect for the elders, filial piety, etc.) and social order is neither achieved nor protected by laws and penalties.

> Laws and punishments imposed from above may indeed promote a superficial social order among the people, but they do little to inculcate in them a sense of right and to lead them to moral betterment.[67]

64 *Regio Decreto 14 gennaio 1923 n. 31 col quale è istituita una milizia volontaria per la sicurezza nazionale*, Gazzetta Ufficiale Storica (Historical Official Journal), http://augusto.agid.gov.it/gazzette/index/download/id/1923016_PNC (visited 27 August 2019).

65 In 2019, both the Hong Kong and Spanish governments approached Apple and Microsoft requesting them to prevent protesters using their platforms to find software helpful to their demonstrations.

66 Confucius, *The Analects*.

67 Gardner 2014: 36–37

This seemingly pacific attitude to public order did not, however, prevent Chinese rulers from the use of force, both in internal[68] and in foreign affairs, when it was considered necessary to (re)establish stability.

> History shows that Confucian pacifism is not a valid description of imperial Chinese foreign policy behaviour. Recent scholarship has exposed the enormous discrepancy between this alleged Confucian foreign policy tradition and the frequency and scale of state violence throughout Chinese history. I will, however, further argue not only that Confucian pacifism is a poor characterization of imperial Chinese practice, but that it did not exist, even in the minds of imperial Chinese rulers, if by Confucian pacifism we mean Confucianism's renunciation or neglect of the role of force. Confucianism, in fact, never renounced force as a legitimate instrument of statecraft for waging 'appropriate wars' in the form of punitive expedition. This observation is as damaging to the claim of Confucian pacifism as is the historical counter-evidence sketched in the preceding section, because it challenges the assumed association of Confucianism with pacifism.[69]

This is not an especially surprising judgement since the evolution of Confucian thinking by Mencius and Xunzhi (the two leading Confucian thinkers) in the 3rd century BC shifted the burden of achieving moral superiority mainly by way of self-cultivation toward the duty of the ruler to encourage, gently, the development of human moral qualities:

> It is the explicit responsibility of the ruler, Mencius argues, to assist his subjects in their efforts to keep to the right path. To this end, the ruler is enjoined, in what is an especially eloquent passage in the text, to provide for the material well-being of his people.[70]

In contrast to Mencius' view that man is by nature evil, Xunzhi adopted a more overtly repressive view of the relationship between ruler and citizen, advocating a more direct and stronger intervention into the individual's attitudes in order to turn his natural fondness for the 'wrong' into the praise of 'true values.'

> Given his view of human nature and the need to 'reform' it, Xunzhi places considerably more emphasis on the role of learning and ritual

68 Chao 1988: 175–189.
69 Feng 2015: 197–218.
70 Gardner, Daniel K., *cit.*: 54.

> principles in the cultivation process than does Mencius. Learning and rituals are essential tools in acculturating man, in reshaping his recalcitrant nature.[71]

Although Mencius' views superseded those of Xunzhi, the doctrinal contrast between the two major traditional Confucianism scholars reveals the need to ensure citizens live in a state of peace, even if this necessitates a degree of forceful intervention. In other words, the preservation of power is achieved either by gentle persuasion or coercion to 'self-comply' with the moral values embodied in the ruler. On an abstract level, the Confucian approach may be summarised by describing its emphasis on the rule of ethics attained by a strong system of rituals. This reduced the need to rely upon laws as a means of social control. The result is a social model where, at least on the surface, there is—to adopt the title of John Haley's renowned book—authority without power.[72] And there is no evidence to suggest that this approach has significantly altered. Confucian ethics regards force as an acceptable military option.[73] Moreover, the use of force is recognised as an appropriate means by which to maintain the social order. In Imperial Beijing

> continuous routine patrol and strictly enforced curfew were crucial in preserving spacial order and preventing crime. Other measures helped order the city population by enforcing a mutual responsibility system in the Outer City and household registration in the Inner, keeping a close watch on traveller and foreigners, and paying special attention to predictable large gatherings.[74]

A century later, Article 7 of the 2009 Law of the People's Republic of China on the People's Armed Police Public order and national security[75] declares that the People's Armed Police Force shall

> Assist public security organs, State security organs, judicial administrative organs, procuratorial organs and judicial organs in performing the tasks of arrest, pursuit, capture, and escort, and assist other relevant organs in performing important escort missions, participate in dealing with rebellions, riots, serious violent and illegal incidents, terrorist attacks and other social security incidents.

71 Ibid, *cit.*: 59
72 Haley 1991.
73 Twiss and Chan 2012: 447–472.
74 Dray-Novey 1993: 895.
75 Law of the People's Republic of China on the People's Armed Police, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620753.htm (visited 10 December 2020).

Moreover, with disturbing ambiguity, the same provision tasks the police to perform 'other security tasks entrusted by the State.'

The continuing crackdown on protests and protesters in Hong Kong by mainland authorities demonstrates the extent to which the Chinese Communist Party is willing to deploy an iron fist in a steel glove. There are several recent instances of heavy-handed police behaviour in Western countries (notably Spain, Italy, and the US), but in China the regulation of social and political activities is increasingly managed by enacting legislation rather than by following tradition or custom. This has less to do with the adoption of the rule of law, and much more with the 'weaponisation' of legislative and judicial power, thereby turning a Western soft approach (laws and rights) against its protagonists.

Public order (or, more accurately, social stability), and national security lie on a political continuum; it is often difficult to determine where one ends and the other begins. Still, three recently passed statutes elucidate this concept of law weaponisation or, as it has been called, 'lawfare.'[76] The Cybersecurity Law came into force in China on 1 June 2017. It affirms Chinese sovereignty over the 'local' network and everyone (including foreign companies incorporated under Chinese law) is obliged to cooperate with the State and judicial authorities in particular. Similarly to the European Union project[77] (and Russia's legislation),[78] this law also requires the retention of data within national borders. Moreover, matching the Western trend of infusing ethics as an ingredient of legislation, Article 9 requires network operators to comply with social standards, to follow business ethics, and to behave honestly and credibly, accepting government controls. This is little different from the position in Western jurisdictions, including the US.

Secondly, the Export Control Law, approved by the Central Committee of the People's Republic of China on 17 October 2020, is essentially the Eastern version of the Wassenaar Treaty regulating the export of dual-use goods, services, and technologies. Consistent with Western principles, Chinese law affirms the right of the State to block or limit the transfer of any 'object'

76 Goldenziel, Jill I., *Law as a Battlefield: The U.S., China, and Global Escalation of Lawfare* (January 25, 2020). Cornell Law Review, Vol. 106, 2020, http://dx.doi.org/10.2139/ssrn.3525442.

77 European Institute of Innovation and Technology *New Report on European Digital Infrastructure and Data Sovereignty*, 9 June 2020, https://eit.europa.eu/news-events/news/new-report-european-digital-infrastructure-and-data-sovereignty (visited 10 December 2020).

78 Article 2 of the Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions) makes it mandatory to store 'within the Russian Federation, of databases used to collect, record, systematize, accumulate, store, clarify (update or modify), and retrieve personal data of citizens of the Russian Federation.' https://pd.rkn.gov.ru/authority/p146/p191/ (visited 10 December 2020).

that can be used for both civil and military purposes and, in particular, those that increase the military potential in the design, development, construction, and use of weapons of mass destruction and their means of delivery. Article 2 identifies those who have to comply: citizens, legal persons, 'non-corporate organizations.' Article 9 allows the temporary extension of the controls (and therefore the export ban) to goods not included in the list of those subject to verification. Similar to the Cybersecurity Law, the law on exports refers to the concepts of national interest and security, whose definitions—it is worth repeating—are as vague and ambiguous as their Western counterparts.

Thirdly, the draft data protection law[79] has been open to consultation since 21 October 2020. In perfect symmetry with the GDPR, the draft extends the reach of Chinese jurisdiction outside national borders as soon as citizens' personal data are processed abroad. Unlike the EU legislation, however, processing based on the 'legitimate interest' of the data controller (a category that is problematic in Europe) is forbidden. On the other hand, the obligation to locate data in Mainland China is expanded, and the State gains the authority to exert control over data transfers abroad. Offences and sanctions are also in line with those adopted by the EU.

Once again, taken at their face value, these principles are largely consistent with those practised in liberal democracies. A superficial reading would therefore suggest that China is slowly progressing towards the integration of its regulatory system with the European and Western infrastructure and in particular with the rule of law. Closer scrutiny, however, reveals a different story. Firstly, as already pointed out, the Chinese approach to regulation is to adjust the law to the political needs of the Party rather than conceiving it as an insurmountable limit even to established power. Not the rule of law, therefore, but rule *by* law.[80] Secondly, it is clear that the Chinese legislator employs legal design techniques similar to their Western equivalents. It is undoubtedly the case that 'vague concepts of national security and public interest increase the possibility for the government to support the need for controls and reduce the ability of a foreign company to challenge a request for access to the data it holds.'[81] It is also true, however, that these concepts are no less vague when used in Western legislation, and that national security and the public interest are also deployed by the US and European countries to justify political choices and operational decisions.

Finally, and once again transposing principles largely imposed by political necessity in Western nations, China affirms its right and power to apply

79 Cao Siqi and Chen Qingqing, 'China Unveils First Law on Personal Data Protection,' *Global Times* online edition 13 October 2020, https://www.globaltimes.cn/content/1203363.shtml (visited 10 December 2020).

80 Monti and Wacks 2020: 125. See generally Wacks 2021b.

81 Wagner 2017.

its laws outside its borders, not unlike the GDPR, or what individual countries seek to do with the creation of the 'web tax' which, for purely political reasons, alters the consolidated principle of the territoriality of the fiscal imposition.

Although unacceptable at first blush, these Chinese statutes are perfectly in line with the Western approach. They establish national sovereignty over physical resources and data located in China, impose duties of cooperation with the authorities, and are effective beyond its borders. As a result, not only foreign companies that are based in China, but also those that process the data of Chinese citizens outside their borders are within the reach of the executive arm of the government. This implies, therefore, the possibility of Western subjects being caught up in complex and difficult disputes, rooted in a system that is not subject to the rule of law.

This is yet another demonstration of what transpires when the law is transformed from a means by which to settle political disagreement to a political tool or weapon.

In practical terms, evaluating the Spartan Xenelasian law, and the other methods of achieving public order described in this chapter, it is hard to avoid the conclusion about—from a modern perspective—what the ancient rulers had in mind, when they sought to protect the 'harmony of the State' and 'good manners' while deterring 'bad habits.' Each, to a greater or lesser extent, had in mind the very same approaches that came to be espoused by the great European States.

Italy has adopted a more abstract, citizen-oriented approach to the definition of public order, although beneath the surface of the convoluted legal language, signs of the British approach are evident.[82]

Whether it is the approach of the Romans[83] or the influence of neo-Confucianism in the Far East,[84] it is clear that at the heart of all structures that seek to protect and defend public order and national security lies the reality

82 Italy shifted the fascist definition (and function) of public order as a tool to repress political dissent to a constitutionally grounded definition. This process, which took more than 60 years, ended in 1988 when the Italian Constitutional Court held that public order (*Ordine Pubblico*) must be understood as 'all the fundamental legal assets or primary public interests on which, according to the Constitution and ordinary laws, the orderly and civil coexistence of the associated companies in the national community is based. These functions, therefore, are characterized by being primarily directed to protect fundamental goods, such as the physical or mental integrity of persons, the safety of possessions, public faith and any other legal asset that the system considers, at a given time in history, of primary importance for its existence and its operation.' Corte Costituzionale, sentenza 1013/88 of 26 October 1988, http://www.giurcost.org/decisioni/1988/1013s-88.html (visited 28 August 2019). Unofficial translation by Andrea Monti.

83 Nippel 1995.

84 See Haley 1991; Sheldon 2005; Xuezhi Guo 2014; Paramore 2016.

that its overriding object is the preservation of power rather than the welfare of citizens.

The creation of a specific police entity separate from the military is a relatively recent phenomenon, as is the later political and administrative separation between internal and external security:

> Modern societies have become accustomed to specialized law enforcement agencies called police that are authorized to regulate social conflicts, if need be, by employing physical force. They represent the state's claim to the 'monopoly of legitimate physical violence' (Weber 1972: 29, 183, 516) with respect to internal relations, whereas the army does the same with respect to the outside world.[85]

The pervasive recognition in many advanced democratic societies of the rule of law and separation of powers has generated other distinctive characteristics in public order management. Prevention and repression, the two components of internal security, are no longer controlled by a single administrative body. Police forces are now tasked to ensure that crimes, public disorder, and threats to safety and security are anticipated and dealt with to re-establish order and peace. The judiciary is empowered to sanction criminal activity or to ensure that ordinary citizens' activities are carried out in compliance with the general principles established by the State (business and family relationships, divorce, abortion, and so on).

In regard to external threats, the military has lost the monopoly on intelligence activities so, while still maintaining its own information management apparatus, new administrative entities—loosely called 'secret services'—are charged with the responsibility to gather whatever information is perceived to be necessary for the survival of the State. Intelligence, however, has rapidly advanced beyond the traditional '007 approach,' as State security needs have been merged with the need to control the impact of economic activities in specific critical sectors such as energy and telecommunications in the interests of the State.

In summary, a progressive depersonalisation and abstraction process has, at least in theory, improved the application of democratic checks and balances in the domain of State-manned security. Technically, from the early kingdoms to contemporary republic-disguised empires, 'security' and 'order' have morphed from goals to be achieved by way of the attribution of specific tasks to individuals or institutions, into a cluster of concepts: 'public order,' 'public safety,' 'national security,' and 'national interest,' whose ambiguities and imprecision it will be the task of the following chapter to elucidate.

85 Nippel: 1.

2

PUBLIC POLICY, NATIONAL SECURITY, AND THE RULE OF LAW

... consequentia nomina rebus esse studentes.

—Justinian[1]

The Emperor Justinian foreshadowed the Bard's aphorism that 'a rose by any other name would smell as sweet.' But, as George Orwell observed, echoing King Lycurgus' attitude toward 'foreign things,' controlling words and meaning imposes control over ideas and simplifies the enforcement of public policy choices:

> The purpose of Newspeak was not only to provide a medium of expression for the world-view and mental habits proper to the devotees of Ingsoc, but to make all other modes of thought impossible … It was intended that when Newspeak had been adopted once and for all and Oldspeak forgotten, a heretical thought—that is, a thought diverging from the principles of Ingsoc—should be literally unthinkable, at least so far as thought is dependent on words.[2]

The meaning of words and their interpretation have implications that extend well beyond the page. 'Public policy,' 'national security,' and especially the 'rule of law' require careful definition if they—and the relationship between them—are to be properly understood and analysed. The clash between Shakespeare and Big Brother—or between Socrates and Gorgias—is inescapable: words maketh (political) truth.

A military intervention in a foreign country may be styled as an 'international police operation,' but when it is launched by the military, in the absence of legal control or regulation, it is simply 'war.' Similarly, a new political initiative to discourage the use of private vehicles by raising fuel

1 'We are trying to make words match things.' *Institutions* II.7.3, 533 AD.
2 Orwell 1949: 236.

DOI: 10.4324/9780367809775-2

prices may be dubbed 'green,' but it may simply constitute the imposition of new taxes.[3] Alternatively, it may be maintained that a motorcycle gang is not part of the enforcement of a political strategy. The claim does not render it true.[4]

Such claims are simply that; they express reality according to a specific political interest. And this is no less true in regard to the definition of public policy and its relationship with national security and the rule of law:

> Ruling is an assertion of the will, an attempt to exercise control, to shape the world. Public policies are instruments of this assertive ambition.[5]

This definition helpfully elucidates the relationship between power and policy: the former precedes the latter. In other words, if there is no (self-protection of) power, there is neither public policy as a system of political goals, nor public policy as an instrument of enforcing that power. It is therefore, we suggest, accurate logically and factually to describe the preservation of power as the primary motive of public policy goal-setting.

In the opposite corner of the ring sits the rule of law, the other contender in the struggle for managing the State, whose role is to prevent the exercise of public policy from destroying the checks and balances that preserve the operation of democratic governance. Over time, depending on the strength of these two fictional pugilists, the bouts favour one or the other, but rules (admittedly, more similar to pre-Broughton Rules than to the Marquess of Queensberry's code) are nevertheless established and respected. Moreover, if we exclude from this analysis the possibility of a *coup* as a route to untrammelled power, we must conclude that public policy must account for the rule of law without exceptions. This tension, as discussed in Chapter 1, demonstrates that the sheer will of a ruler is insufficient to elicit compliance from the ruled. Persuasion, or better still, propaganda, is required to ensure that the Pied Piper is followed.

3 Towards the end of 2019, the Italian government announced its 'green economy' plan which included raising taxes on plastic bottles and diesel fuel. Critics say that the 'green economy' was just an *escamotage* to justify the increase of fiscal pressure, which the government denied. Bassi, Andrea, Dimito, Rosario. 'Manovra, stangata sul diesel con il taglio alle agevolazioni. Stop di Conte al ticket.' *Il Messaggero* online edition, 3 October 2019, https://www.ilmessaggero.it/politica/manovra_diesel_manovra_2020_diesel_macchine_tassa_news-4772933.html (visited 10 January 2020).

4 Peter Laurence, 'Slovakia Alarmed by pro-Putin Night Wolves Bikers' Base.' *BBC News* 31 July 2018, https://www.bbc.com/news/world-europe-45019133 (visited 10 January 2020).

5 Moran, Rein, and Goodin 2008: 3.

Historical precedents

Rulers of the past had to rely upon might, gods, and *mores* to pursue their objectives. Their contemporary heirs generally deploy more sophisticated techniques to achieve the same ends. The core of the matter, however, does not change: power needs to provide citizens with a reason or an incentive to comply, the less logical or fact-based, the better.

Edward Bernays offers the best synthesis of the conundrum that strips meaning from the term 'democracy':

> The conscious and intelligent manipulation of the organized habits and opinions of the masses is an essential element in a democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the real ruling power of our country … In almost every act of our daily lives, whether in the sphere of politics or business, in our social conduct or our ethical thinking, we are dominated by the relatively small number of persons—a trifling fraction of our hundred and twenty million—who understand the mental processes and social patterns of the masses. It is they who pull the wires which control the public mind, who harness old social forces and contrive new ways to bind and guide the world.[6]

Bernays' assessment is a well-established position in the field of public policy studies. It would not need to be developed further, but for two facts: firstly that *persuasion* of the ruled is something intrinsically linked to the exercise of power, no matter the technological or social stage of political and economic evolution and, secondly, that power does not reside in the sole hands of the king. History bristles with examples of non-ruling actors who had a firm grasp on the official sources of power until that power decided to get rid of them.

So, for instance, the history of the 'medieval super-companies' (as the banks belonging to the Florentine family of Bardi have been called)[7] is revealing. In the first half of the 14th century, the Bardi and the Peruzzi, another Florentine family, were owners of the two most prominent banks in Europe that financed massive local and foreign military campaigns. The two-year-long struggle between Florence and the rulers of Verona, the *Scaligeri* (between 1336 and 1338 AD), cost the *Comune* of Florence some 450,000 *Fiorini* (about a ton and a half of gold), and the war against the city of Lucca raised the debt to 600,000 *Fiorini*.

6 Bernays 1928: 9–10.
7 Hunt 1994.

As in a modern financial system—or a Ponzi scheme—until the debtor promises to repay the debt, the wheels keep turning. But when the debtor changes his mind, the whole machine crashes. This happened in 1341 when King Edward III of England refused to repay the loan of 900,000 *Fiorini* (about three tons of gold) that he had incurred to wage war against France. Although there are doubts about the actual extent of the king's debt,[8] the impact of his decision not to honour it, and the speculation that the real cause of the bankers' bankruptcy was the city of Florence's default,[9] the fact is that a sovereign decision not to respect the rules was the root of the financial crisis.

The fate of another non-State actor, this time a military enterpriser, tells the same story. In the early 17th century, Albrecht Wenzel Eusebius von Wallenstein was a successful *generalissimo* whose services (and army) were purchased by the Holy Roman Emperor Ferdinand II, making him the richest man in Europe. His power and wealth did not, however, spare him from death at the hands of the emperor himself.

According to the agreement between the emperor and Wallenstein, the cost of the latter's army would be covered by taxing the Hapsburgs' lands which would also provide (together with other allied territories) equipment and new recruits.

In the winter of 1633–1634 AD, the emperor ordered Wallenstein to launch a campaign against the Swedish army stationed in the adjacent German territories.

Wallenstein's generals refused to follow the order while, at the same time, they swore allegiance to their commander. Their reason for refusing to fight was that waging war in the harsh winter climate

> would jeopardize access to finance and supplies essential for the recruitment and re-equipping of the army … bringing with it the recognition that the financial base of the army was fragile and could only be neglected at high risk.[10]

Wallenstein's enemies labelled these mundane financial concerns as treacherous and succeeded in having Wallenstein killed in the implementation of the emperor's 'executive order.'[11]

Wallenstein's case was not an isolated one, as in the world of military entrepreneurship 'employers often made it treasonous for able enterprisers to abandon their contracts and had the power to enforce this clause,

8 Sapori 1926: 77.
9 Hunt 1990: 149–162.
10 Parrott 2012: 121–122.
11 Ibid.

causing the enterpriser to lose both fortune and head.'[12] It is true that the relationship between the employer (a ruler) and the employee (the military entrepreneur) relies upon an agreement, i.e. upon the law. Nevertheless, it was an act of power, rather than a court decision on a claim for breach of contract, that decided its fate. Yet again, the needs of the powerful override a binding legal agreement.

These are but two examples from the many that could be mentioned. They reveal the true nature of the question posed in Chapter 1: are those in power bound to comply with the law?

Policy and power

The distinction between principles and policies, advanced by Ronald Dworkin, is helpful in this connection. A 'principle' is 'a standard to be observed, not because it will advance or secure an economic, political, or social situation, but because it is a requirement of justice or fairness or some other dimension of morality.'[13] A 'policy,' on the other hand, is 'that kind of standard that sets out a goal to be reached, generally an improvement in some economic, political, or social feature of the community.'[14]

But in the present context it is clear that policies express the will of the ruler. Principles—or rights—are a concession made by the ruler; they are therefore, in effect, a component of the public policy architecture. The law is thus merely one of the various instruments by which the ruler's policies are executed. Nor does the scenario change with the acknowledgement of the existence of, or, better still, the political choice to recognise human rights, a contemporary version of the 19th-century octroyed constitutions. This is a key point because—as argued in Chapter 1—it marks the boundary between the rule *of* law and rule *by* law. It also differentiates a liberal system from an authoritarian regime.

At least in theory, at the international level, the political arrangement manifested by the United Nations requires members to act, or to refrain from acting in any way that would endanger these rights. Their ubiquitous recognition and expression by many constitutions, bills of rights, and judicial decisions around the world has not, however, prevented their breach by numerous governments when national security, the 'national interest,' or the vague concept of 'market regulation' is claimed to be imperilled.

12 McFate 2015: 30.
13 Dworkin 1985: 22.
14 Ibid. See Wacks 2021a: Chapter 5.

The case of the European Union's Charter of Fundamental Rights (the Charter of Nice)[15] is paradigmatic. Signed in 2001, it is the closest approximation to a European constitution considering the rejection of the proposal to establish direct sovereignty over member States' own constitutions. This political expedient afforded the EU a *de facto* constitution, for it has become the basis of the European Court of Justice's jurisdiction, and for the operation of other European institutions. While the historical circumstances that gave birth to the Universal Declaration of Human Rights might offer some evidence of its intent, the same cannot be said for the Charter of Nice. Critics have remarked that the Charter was intended less as a 'shadow' constitution than as a market stabiliser:

> [T]he Charter, whether intentionally or not, bears the sign of an 'instrumental effect' necessary to the functionalist principle, whose objective, in these respects, is the structuring of an 'environment of rights' compatible with the efficiency of the markets and competitiveness, by means of minimum models of uniformity and standardisation, such that if a State were to fall below them, the performance of businesses would be drugged and competition distorted. In essence, it is a matter of guaranteeing a nucleus of rights and, at the same time, preserving the unity of the market from the variability of the national regulatory contexts, especially future ones, with a view to the entry of new countries into the Union.[16]

In this reading of the role of human rights (or 'fundamental rights' as the Charter calls them), they chiefly serve the interests of member States; the (positive) benefits for the citizen are merely collateral side effects. The disagreement between the European Union and two of its member States, Poland and Hungary, is a vivid demonstration of this observation:

> The leaders of Hungary and Poland have vowed to maintain a united front and uphold their veto of the EU's budget and its massive pandemic relief fund. They continue to oppose the mechanism that ties funding for countries to rule of law principles, arguing that the EU plan risks derailing the bloc.[17]

15 Charter of Fundamental Rights of the European Union. (2000/C 364/01) Official Journal of the European Communities C 364/01 18 December 2000, https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

16 Di Plinio 2001: 152.

17 Sandford, Alasdair, 'Hungary and Poland Maintain United Front Blocking EU COVID-19 Recovery Fund.' *Euronews-World* 27 November 2020, https://www.euronews.com/2020/11/26/hungary-and-poland-maintain-united-front-blocking-eu-covid-19-recovery-fund (visited 11 December 2020).

Is the EU weaponising human rights in pursuit of its political agenda?

Laws, when not overtly overridden, are 'massaged' to meet the (democratic) kings' will, and human rights have become a new weapon in the arsenal of the powers-that-be. They can be used by a parliamentary minority to counter government policies, or by a government to lure parliament into a war, or by the now 'free' citizens of the contemporary third estate to reclaim their 'rights.'

There are in Europe numerous examples such as the 2020 demonstrations in France, where violent riots occurred in the *boulevards* of Paris and forced Prime Minister Edouard Philippe to 'temporarily' withdraw his pension reform project.[18] Another instance is the 2019 Barcelona riots opposing the Catalonian 'independentists.' Or 'the Troubles' in Northern Ireland which abated in 1998 and concluded in 2007.

The rule of law is not always welcomed by those in power. Scholars have expended considerable effort to devise means by which to free political activity (and, thus, public policy) from its constraints or to reframe the concept so as to subordinate law to politics. 'National security' is perhaps the most effective *passepartout* to pursue this goal. To take an example from Italy, in his theory of the 'material constitution,' Costantino Mortati, professor of public law and member of the parliamentary assembly that in 1948 drafted the Italian Constitution, and later a member of the Constitutional Court, was adamant in affirming that a constitution is the outcome of the will of the ruling party.[19] By implication his theory plainly acknowledges the considerable incongruity between public policy and the rule of law. This divergence reached its zenith in a paradoxical situation where both statesmen and terrorists refused to concede the right and the power of the State to try them for breaking the law.

On 28 April 1977 Fulvio Croce, president of the Turin Bar and defence counsel for the members of the extreme left Red Brigades terrorist group, was killed by one of their number who had yet to be apprehended. On 3 May 1977 Red Brigatist Maurizio Ferrari read the following statement in court admitting the murder:

> We publicly proclaim ourselves militants of the communist organization Red Brigades, and as communist fighters, we collectively take full political responsibility for all its past, present and future initiatives. By affirming this, any legal prerequisites for this trial have been removed, and the defendants have nothing to defend themselves against. On the contrary, the accusers have to defend

18 BBC News, 'France Protests: PM Offers Pension Compromise in Bid to End Strike.' 11 January 2020, https://www.bbc.com/news/world-europe-51078405 (visited 11 January 2020).
19 Mortati 1940.

> the criminal, anti-proletarian practice of the infamous regime they represent. If there are to be defenders, then you need them.[20]

Seventeen years later in 1994, former Italian prime minister and secretary of the Italian Socialist Party, Bettino Craxi, a self-proclaimed victim of political persecution, took refuge in Tunisia to escape the investigation that led to the party's conviction for corruption. Thus, though the individuals represented different political positions, we see the same State, the same law, and the same relationship between power and rights. Moreover, to complicate matters, power is exercised other than by the formal institutions of State (the legislative and executive), but from a different source, as Edward Luttwak remarks in his essay on how to organise a *coup*:

> [T]he seizure of the supposed political center will not win the battle; the sources of political power may be in other centers that may be too difficult or too numerous to seize. And so the realities of power are in conflict with the theoretical structure of the state, just as in those cases where the political unit is not truly independent. Here, 'power' exists within the country—but it is not where it is supposed to be because the political entity is not really organic.[21]

The decline of the rule of law?

Furthermore, it should be acknowledged that constitutionalism, the legal theory that supports the rule of law, has an intrinsic, and increasingly waning, connection with national borders and jurisdiction. In other words, the long unchallenged assumption is that the State, even though democratic, remains the absolute form of power as it emerged after the 1648 Peace of Westphalia. This assumption is no longer accepted without criticism; several scholars point to the fact that States have lost their most important attribute: the monopoly of force and power.[22]

In a striking analogy with medieval times, where fragmented powers resided in the hands of a large group, the current condition has been labelled 'neomedievalism,' i.e. a condition based upon

> a non-state-centric, multipolar international system of overlapping authorities and allegiances within the same territory … States will not disappear, but they will matter less than they did a century ago. Nor does neomedievalism connote chaos and anarchy; like the

20 Merlo 2017.
21 Luttwak 1968: 36.
22 Khanna 2009; Duran 2019; Berzins & Cullen 2003; McFate 2015.

> medieval world, the global system will persist in a durable disorder that contains rather than solves problems.[23]

Furthermore, as McFate comments, States have lost their centrality in the international order, and are in direct competition with multinational companies, international institutions, and non-governmental organisations.

In other words, the national State ideal, whose founding social contract is the exercise of power as a *quid pro quo* for the care of the security, safety, and well-being of the citizen, is not there anymore, as we are experiencing a transition to a form of market State:

> The globalization of markets, owing to advances in computation, invites the rapid transience of capital, reduces the autonomy of the nation-state to manage its own currency and economy, and encourages rapid economic growth that has transnational consequences like climate change and inequality … Rather than attempting to control behaviour through prohibitory regulation, the State will devise incentives for individual choices that generate positive spillovers and externalities.[24]

The decline of governmental power has increasingly placed the reins of public sector in the hands of private, supranational entities that control every aspect of our Matrix-like existence. The choice of major software multinationals to support a specific piece of software directly affects public spending.[25] New computer programmes or hardware components must be purchased not because they are necessary, but 'just' because an independent actor created the need according to its own business plan. A major Far East private high-tech manufacturer owns the keys that open the doors to the realm of 5G technology, but it is then regarded as a 'threat to national security.' The subsequent refusal to purchase this equipment inevitably delays the adoption of a technological breakthrough and retards modernisation.[26] Pharmaceutical companies develop a coronavirus vaccine but, in those countries where they do not already enjoy such protection,[27] seek immunity from legal liability.[28]

23 McFate 2015: 73.
24 Bobbitt 2018: 1832.
25 Wright 2020.
26 Monti 2020a.
27 US Congress *Public Readiness and Emergency Preparedness Act of 2005* https://www.hrsa.gov/sites/default/files/gethealthcare/conditions/countermeasurescomp/covered_countermeasures_and_prep_act.pdf (visited 12 December 2020).
28 Lintern 2020.

As a consequence of the interconnected economy paradigm, we have elevated companies to the status of a State, or we have demoted States to mere players in the market. The referee has lost his independence and now competes with those whose conduct he was supposed to control. It would be simplistic to describe this as a global plot aimed at establishing a 'New World Order' run by a congregation of cold-blooded entities hiding their nature behind a human appearance. And it would be idealistic to expect 'global nationalization' of natural resources and knowledge. In this scenario, can we still rely upon the rule of law as a fundamental concept to manage the domestic and international order? If not, upon what principles ought the State's public policy and law to be based?

Slogan or standard?

What is the rule of law? Its promiscuous use has undoubtedly undermined its value, and perhaps even thwarted its effective defence. It has grown into a nebulous notion that benefits both its supporters and detractors. Of course, a generous 'rule of law' accommodates a wide variety of constitutional norms, but without elements that are sufficiently distinctive, coherent analytical identification and description are hampered and its prognosis is weakened. It may be replied that subscribing to generalised values exhibits our commitment to them, but it seems perverse not to attempt to refine the nature and scope of the concept, especially if this might actually engender more effective protection. When an idea degenerates into a slogan, the prospects of it being properly understood, applied, or recognised are weakened.

Form or substance?

This is not the place for a detailed exegesis on the rule of law[29]; suffice it to say that the concept dates back to ancient times, and that there is a long-standing divide between those who adopt a formal or procedural view of the concept, on the one hand, and the theorists who vest the notion with substantive moral content, on the other.[30] The former position is most closely associated with the Victorian constitutional theorist, A.V. Dicey, who famously formulated three principles that stipulate the necessary institutional and constitutional requirements without specifying what the content of the law ought to be. The first declares that

> no man is punishable or can be lawfully made to suffer in body or goods except for a distinct breach of law established in the ordinary

29 See generally Wacks 2021b.

30 For an illuminating discussion of the moral argument, see Simmonds 2007.

> legal manner before the ordinary courts of the land. In this sense the rule of law is contrasted with every system of government based on the exercise by persons in authority of wide, arbitrary, or discretionary powers of constraint.

This principle embodies the important prerequisite that the laws under which individuals are punished should be enacted in accordance with proper legal procedures, and that guilt should be established only through the normal trial process. Dicey's reference to wide, arbitrary, or discretionary powers might extend to laws that violate certain fundamental rights, or it might describe laws properly enacted, but which are vague or uncertain so that citizens are unable to plan their lives in harmony with the law.

The second principle asserts that 'every man, whatever be his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of the ordinary tribunals.' This upholds the importance of equal access to the courts. This is again a formal or procedural idea rather than a substantive concern with how judges actually apply the law to different individuals or social groups. The principle is therefore not incompatible with discrimination or special treatment.

'We may say,' Dicey stated thirdly,

> that the [British] constitution is pervaded by the rule of law on the ground that the general principles of the constitution (as for example the right to personal liberty, or the right of public hearing) are with us the result of judicial decisions determining the rights of private persons in particular cases brought before the courts.[31]

This is a claim of superiority of the British unwritten constitution over those written constitutions of continental Europe. For Dicey, individual liberty was more secure where it was the product of judicial decision rather than being susceptible to repeal or abrogation by authoritarian governmental fiat.

Legal theorists in several countries have sought to adapt the conception of the rule of law to contemporary questions of legality, authority, and other virtues of democratic governance. In his examination of what he dubbed the 'inner morality of law,' Lon Fuller specifies eight desiderata with which the law should comply if it is to achieve 'excellence.' A legal system, he argues, is the purposive human 'enterprise of subjecting human conduct to the guidance and control of general rules.'[32] Whatever its substantive purpose, a legal system is bound to comply with certain procedural standards.

31 Dicey 1885.
32 Fuller 1969: 106.

In the absence of this compliance, what passes for a legal system is merely the exercise of State coercion.

His eight desiderata or 'eight kinds of legal excellence toward which a system of rules may strive'[33] are generality, promulgation, non-retroactivity, clarity, non-contradiction, possibility of compliance, constancy, and congruence between declared rule and official action. Where a legal system does not conform to any one of these principles, or fails substantially in respect of several, it could not be said that 'law' existed in that community.

Joseph Raz attempts to add flesh to the bare bones of Dicey's principles, while stressing that the rule of law is not the sole virtue of a legal system.[34] His organising principle is that the rule of law performs a crucial role in facilitating individuals planning their lives.[35] To do so, he argues, the law ought to be prospective (as opposed to retrospective) and relatively stable; that particular laws should be directed by open, general, and clear rules; that the courts should be independent and accessible; and that those who enforce the law should not have untrammelled discretion.

But a wicked legal system could satisfy these norms (or even Fuller's) while enacting unjust laws.[36] Nevertheless, as Raz insists, a formal (or content-neutral) conception of the rule of law permits us to evaluate the operation of a legal system independently of its political or moral quality. He has recently revised this earlier account to emphasise the rule of law's purpose in preventing arbitrary government. He now claims that the rule of law requires that government action displays the intention to defend and advance the interests of the governed. It therefore becomes an almost essential condition for the law to satisfy other moral demands, and it operates as a co-ordinating force domestically and internationally.[37]

Several writers reject this approach and look instead to the power exercised by the judiciary over the executive. Judicial review is an important means by which government is kept in check and thereby rendered more accountable, both procedurally and substantively. For example, Ronald Dworkin maintains that 'propositions of law are true if they figure in or follow from the principles of justice, fairness and procedural due process that provide the best constructive interpretation of the community's legal practice.'[38] Dworkin places the courts at the epicentre of the legal system. It is their function to decide what rights individuals have. In this endeavour, judges ought to select the interpretation of the law that best fits with the

33 Ibid: 39.

34 Raz 1977 and 2019. See too Gardner 1994; Bingham 2010; Craig 1977.

35 'The rule of law … implies the precept that similar cases be treated similarly. Men could not regulate their actions by rules if this precept were not followed.' Rawls 1971: 237

36 See Wacks 1984a, 1984b, 1991, 1998, 2000, 2009, 2021b.

37 Raz 2019. See Grant 2017.

38 Dworkin 1986: 225.

commitment of the law to justice, and displays the community's institutions in the best light. The formal (or 'rule book') notion of the rule of law, Dworkin contends, neglects the centrality of individual rights; citizens have moral rights and duties with respect to one another, and political rights against the State. Such rights should be recognised in positive law, in order that they can be enforced by the courts. The conception of the rule of law 'does not distinguish, as the rule book conception does, between the rule of law and substantive justice; on the contrary it requires, as part of the ideal of law, that the rules in the book capture and enforce moral rights.'[39]

For the purpose of this book, we adopt a 'thin' construction of the rule of law whose principal function is to restrain the abuse of power by proscribing arbitrary and unfettered discretion, and subjecting all persons to legal rules.

Civil and common law approaches

It is generally true that while at the heart of the continental civilian tradition is the maxim, *ubi ius ibi remedium* (where there is a right there is a remedy), the common law adopts the contrary position (where there is a remedy there is a right). Roman law differentiates *ius* and *lex*.

> It can be agreed that law as the vehicle of a collective ethic and unwritten laws as a dialectical category to positive law are a product of the Greek spirit. However, the invention of ius in the West and the subsequent (whether legitimate or not) authoritarian constraint of public and criminal laws on hermeneutics is an accomplishment of the Roman genius.[40]

Ius—and this is a crucial point—is not simply the outcome of judicial interpretation of the law. It is also a set of principles acknowledged by the legal system and central to its operation.

The common law is less able to achieve the degree of precision, as, say, the German *Grundgesetz* where *Gesetz* (*lex*) and *Recht* (*jus*) are clearly distinguished as a means of containing both executive and judicial power. What impact does this—and related—differences between the two approaches have on the rule of law?

> Common law systems celebrate the Rule of Law … as a legal mythology of the Legality as a supreme regulator, of the subjection of the state (government, ruler) to the law. Moreover they adopt the idea of Common Law collective creation as the beating heart

39 Dworkin 1985: 11–12. See too Allan 2001; Jowell 2000; Endicott 1999.
40 Donini 2019: 9.

> of original legality, the 'rational' synthesis of all the *rationes decidendi*, the most rational possible (and therefore ius!) because they do not represent the will of a single judge or a political party. These systems, however, do not, as we know, have the words to differentiate lex and ius: the provision decided by political power from the rationally controlled norm. And customary law (common law), which is not decided by the political power, is also 'law.'[41]

The hoary debate between natural law and legal positivism cannot be pursued here beyond the brief observations above.[42] Our concern here is to sketch the relationship between the rule of law and the problems raised by the protection of national security.

The rule of law and national security

Difficulties arise when it is sought to recognise an *international* rule of law:

> In this complex (and uncertain) legal environment, one must ask what role the notion of Rule of law can play (and how), once one has to uproot it from the territory of state sovereignty, from the 'domestic' framework of fundamental rights, from the protection of constitutional democracies, and project its normative content into a universe incommensurable with respect to that familiar to it, in which it was formed and cultivated.[43]

Out of the shadow of World War II emerged the notion of 'international legality' based upon 'shared principles' to avoid the horrors of the Holocaust, Hiroshima and Nagasaki, and the ethnic cleansing in the Balkans, Africa, and the Far East. The impulse to punish the offenders reached its zenith in 1998 with the Statute of Rome that gave birth to the International Criminal Court. Although the moral principles that inspired the foundation of the court are fundamentally uncontentious, the US, Russia, China, and Turkey have declined to assent to its jurisdiction.

The reluctance of States to recognise an absolutist notion of the rule of law is hardly surprising in view of the weakening of their role on the international stage:

> [I]mportant values in postnational politics—the need to reflect multiple competing polities and to enable strong contestation—can

41 Ibid: 19.
42 The literature is gargantuan. For an overview see Wacks 2021a: Chapters 1–5.
43 Palombella 2012: 70.

> serve to justify compromises with rule-of-law ideals. This does not make the rule of law meaningless in the postnational order: it continues to represent an important political ideal, only one that does not find an institutional home in the macro-structure of the legal order. It does not lead to an integrated legal order that defines which law rules when, but exerts its influence in a more context-dependent way.[44]

To summarise, on the one hand, an international, principle-based right is created to affirm the existence of what is better called 'supranational' rather than 'international' legality. On the other hand, although States are urged to embrace it, the rule of law becomes rule by law and, as such, expendable on the altar of *realpolitik*: the stronger the rulers, the weaker is their willingness to sacrifice their sovereignty. The risk is that the rule of law becomes a political tool to be manipulated to suit the needs of leaders.

There are numerous current examples of this tendency. We identify a few. Firstly, private multinationals intervene in the political struggles of sovereign countries by supporting the rule of (local) law and preventing access to a piece of software to protesters.[45] The French president, Emmanuel Macron, awarded the Egyptian president the *Légion d'honneur*, affirming at the same time that 'he would not condition the sale of weapons to Egypt on human rights because he did not want to weaken Cairo's ability to counter terrorism in the region.'[46] As in the case of Russia, its history 'provides little evidence of commitment to a universalistic view of law.'[47] In spite of the principle of separation of powers, Malta allowed the executive (not parliament) to appoint judges, and the EU attorney general did not consider it improper.[48]

The Trump administration's hostile relationship with China provides several reasons why the rule of law should not become entangled in political struggles and how, by contrast, that involvement has become a standard operating procedure.

'Privacy, security and social manipulations concerns' are the apparent reasons behind the banning of the (Chinese) platform TikTok in the US.[49]

44 Krisch 2012: 285.
45 McCarthy 2020.
46 Irish 2020.
47 Hendley 2009.
48 European Court of Justice, Press Release 172/20 *Advocate General Hogan: EU Law does not preclude national constitutional provisions under which the executive power or one of its members, such as the Prime Minister, plays a role in the process of the appointment of members of the judiciary* 17 December 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-12/cp200172en.pdf (visited 22 December 2020).
49 Doffman 2020.

Concerns about human rights are cited as the justification the US offered for the banning of the world's largest manufacturer of drones (that happens to be Chinese). It claimed that it permitted the Beijing government to use its products to track political insurgents.[50] But it is when the judicial system is involved in the exposure of hostile intelligence activities that damage to the rule of law is rendered beyond repair. *The Diplomat*[51] reported the confession of two Chinese scientists who pleaded guilty of having 'conspired to steal trade secrets from a medical research center' on behalf of, or for the benefit of, the Chinese government. The article maintains that this was the occasion for the FBI to publicly denounce Chinese espionage activity, which is said to be behind about 60 per cent of similar cases against the US. Moreover, it reported that according to radical organisations belonging to various religious denominations the situation is so critical as to request the inclusion of the Chinese Communist Party on the list of transnational criminal organisations.

Insensible of its own recent history, the US increasingly resorts to the judiciary to deal with cases which are the proper reserve of the intelligence services since they involve national security. Even overlooking the irony that the country owes much of its industrial development to the theft of technology from the UK and other European countries,[52] the reality is that the acquisition of scientific information, or preventing a country—as in the case of Iran—from acquiring it, is a central element in the strategy of any government. Thus, if the cases of industrial espionage discovered by the FBI were, in fact, traceable to the Chinese government, one wonders why, instead of managing them with pragmatic retaliation such as the expulsion of a diplomat or other *persona non grata*, the American administration decided to publicise this news, further harming US–China relations. While it is not unreasonable to wish to punish those who harm us, we are not necessarily justified in inflicting harm as retaliation. Therefore, if the US can legitimately complain about hostile operations attributable to China, it should be prepared to suffer the consequences of its aggressive action against its adversaries.

An exemplary case is that of Jerry Chun Shing Lee, a former CIA agent indicted in the US for revealing to the Chinese government the names of Chinese citizens who, in China, provided information to the US.[53] On the one hand, the sentence rightly indicted an American citizen for having helped a foreign foe. On the other, it acknowledged that the US had built a

50 Shepardson 2020.
51 Girard 2020.
52 Ben-Atar 2008.
53 Montague 2020.

clandestine network in that country to gather information and who knows what else.

Another case of industrial espionage involving the US and (allegedly) China reinforces the point. According to the US Department of Justice, a visiting Chinese researcher was

> charged in a criminal complaint with visa fraud in connection with a scheme to lie about her status as an active member of the People's Republic of China's military forces while in the United States conducting research at Stanford University.[54]

The news was released before her formal indictment. It is difficult to describe China as a champion of fundamental rights, but it is precisely the violation of fundamental rights that Beijing invokes in regard to the charge against one of its citizens. There is an exquisite paradox in the fact that the world's leading democracy denounces an individual as guilty before trial, while the archetypal authoritarian regime invokes respect for fundamental human rights!

The manner in which these two nations approached the (geo)political communication regarding Beijing's alleged responsibility for the spread of the coronavirus is less than edifying. President Trump chose to blame China for having caused the pandemic and keeping it secret. For weeks, the world's media reported the accusation as if it were fact. In a thunderous speech, US Secretary of State, Mike Pompeo, declared:

> Today we're all still wearing masks and watching the pandemic's body count rise because the CCP failed in its promises to the world. We're reading every morning new headlines of repression in Hong Kong and in Xinjiang.[55]

The unashamed politicisation of the pandemic sidestepped the need to invoke 'acts of faith'[56] or rely on the 'confirmations'[57] of friendly countries.

54 US Department of Justice, US Attorney Office, Northern District of California Press Release *Visiting Stanford University Researcher Charged with VISA Fraud* 20 July 2020, https://www.justice.gov/usao-ndca/pr/visiting-stanford-university-researcher-charged-visa-fraud (visited 13 December 2020).

55 US Secretary of State *Communist China and the Free World's Future* Speech given at The Richard Nixon Presidential Library and Museum, 23 July 2020, https://it.usembassy.gov/communist-china-and-the-free-worlds-future/ (visited 13 December 2020).

56 ABC *This Week*, 'China's Coronavirus Response Was a "Classic Communist Disinformation Effort"': Pompeo – Martha Raddatz interviews Secretary of State Mike Pompeo, 20 March 2020, https://abcnews.go.com/ThisWeek/video/secretary-state-mike-pompeo-70478299 (visited 12 December 2020).

57 Markson 2020.

The 'fact' is now established. There is no need for either 'evidence' or 'judgments' to consider 'true' what 'everyone knows.' There is no need for the rule of law to obtain. Nor is this unusual; the rule of law does not constrain the media; outside of the courts neither the media nor governments are required or expected to follow the strictures that limit scoops or political arm wrestling. China, on the other hand, resorted to a low-intensity, high-pressure fact-checking strategy. Official denials were flanked by more subtle forms of propaganda, such as the release of a calculating video entitled 'Once upon a virus.'[58]

In short, the Chinese response to the US allegation was based largely upon an escape from the attack by constructing a narrative that reduced the American accusation to a 'fairy tale.' In addition, a new narrative was designed to redirect the attacks towards the attacker so as to make it appear as inconsistent as the accusations it makes. A change of interlocutors is also in place: the US speaks to China, China speaks to Americans. Finally, the use of non-verbal communication techniques increases the overall effectiveness of the response.[59] The risk in this sort of analysis is 'over interpreting' the messages, searching for meanings where, in reality, there is no explicit agenda. Even when faced with a reasonable sounding analysis, it is advisable to adopt a sceptical view. Yet, despite that, it is fairly unlikely that in the soft war between the US and China, PsyOps—psychological operations—play a secondary role. And so, like the devil of Roger 'Verbal' Kint, it makes sense to believe that his greatest deception was to make the world believe that he did not exist.

The rule of law and politics

It is hard to avoid the conclusion that the game of choice is to politicise fundamental rights and the rule of law. This has serious consequences for the relationship between the rule of law and national security as is manifest in the case of the coronavirus pandemic. In many countries, although not with the same intensity, the emergency measures led to a situation very similar to Fraenkel's state of exception. Governments 'seized the moment' by a (not so subtle) manipulation of the public based on nudging techniques.[60] Either, as in Italy, the executive resorted to ham-fisted, bureaucratic, and

58 New China TV *Once Upon a Virus* 29 April 2020, https://youtu.be/Q5BZ09iNdvo (visited 20 December 2020).
59 Monti 2020.
60 Monti and Wacks 2021: 21; Wacks 2021b.

obscure legislation—legislative chaos. Or, as in Poland,[61] Hungary,[62] and Romania,[63] owing to the need to contain the dissemination of fake news about the contagion, there was a crackdown on freedom of speech and other fundamental rights.

The *fil rouge* connecting the exploitation of the COVID-19 pandemic for political goals is the recourse to existing legislation. Governments do not need to conduct a *coup* or 'fix' an election. They need only deploy a formal notion of the rule of law, suitably 'massaged' by the necessity to protect 'national security.'

Is this what is happening to Western democracies? Are they turning from a rule-based system into one based on might and naked power? As disturbing as it may sound, there are several reasons to support the notion that the conventional approach to the rule of law neglects or even ignores fundamental questions about the integrity of the institutions of government. In principle, there is no issue with the general idea that no-one is above the law or that all are subject to the same law, but unless the institutions themselves have integrity and generate trust, the rule of law becomes little more than a slogan.

The classic refutation of this argument is that it concerns political or legal philosophy. By contrast, in real geopolitical scenarios ordinary rules can and must be adapted or violated (paradigmatic is the case of espionage) in the name of the national interest. Such a refutation, though, is unconvincing mainly because of its political ineffectiveness. Building values to unite a nation is an essential element in buttressing the work of the political class in respect of both domestic and foreign policy. In this latter regard, the issue is relevant in at least two areas: that of the international position of a given country, and the type of relationship that is established within an alliance in balancing the national interest and the object of any coalitions. The two may not necessarily coincide.

Ensuring the vitality of the rule of law is an effective unifying element, precisely because of its 'transversality' rather than 'universality.' Not being tied to specific or particular interests the rule of law can more easily represent the 'common ground' which justifies and sustains the existence of a political, economic, and military alliance. In other words, preserving the sacrality of the rule of law is not an abstract, spiritual, or religious matter. It is a pragmatic method by which to pursue shared goals by offering values whose recognition and protection need not diminish governmental power.

61 Reuters Staff *Human Rights Watch Warns against Polish Abortion Debate* 14 April 2020, https://www.reuters.com/article/health-coronavirus-poland-abortion-idUSL5N2C21E7 (visited 20 December 2020).

62 Gall[illegible]0.

63 Jovi[illegible]020.

This, of course, requires a genuine commitment to its precepts. As Luke warned, evil demons cannot be fought by becoming like them (Luke 11, 15–26). Moreover, there is a moment when the dark grey world of political skirmishes surfaces. It can happen because of a calculated move, a required institutional decision, or to ensure that citizens approve a specific course of action. In a nutshell, if the rule of law is a symbol of the free world, it should transcend political haggling.

The rule of law and emergencies

Aside from the effects of these global forces, the 'war on terror' and natural disasters and pandemics, there is yet another blow to the conventional roles of public policy and the rule of law: the loss of boundaries between the different domains in the exercise of power in order to safeguard 'national security.'

The traditional four-part division in the enforcement of power sees the military responsible for defence; the intelligence services as an information-gathering machine; law enforcement authorities to prevent crime and disorder; and the judiciary to administer the criminal justice system. A complex check-and-balance mechanism ensures, at least in democratic countries, that limited overlapping occurs between these branches of government. The military may not supervise internal public order and public security. Law enforcement may not intrude into the area reserved for the intelligence services. And the judiciary must operate under the rule of law and therefore may not request the military to act as their secular division.

In practice, of course, natural disasters—earthquakes, floods, wild fires, pandemics—frequently require the assistance of the armed forces. A good example of how an emergency alters the niceties of constitutional theory is Hurricane Katrina that devastated the states of Florida and Louisiana in 2005. It was not only the army that exercised internal security and crime-fighting duties, but law enforcement officers were deputised by the State governments because of their failure to restore law and order. On the other hand, the military may be used as a diplomatic asset on the international scenario. The 2011 the Tōhoku earthquake, and the ensuing tsunami that struck the Japanese nuclear plant of Fukushima, saw a massive intervention by the US military deployed in the area to assist the Japanese government, with a corresponding political agenda that led to speculation about a possible improvement in the political relationship between the two nations.

Several countries have passed what can be collectively called 'emergency acts' to deal with the unavoidable overlapping jurisdiction of different organs of the State in cases of natural disasters and calamity. This was necessary in order to remain within the rule of law when the lines between various State actors' duties are blurred.

'National security' and more recently 'the war on terror' are, however, entirely different. Using the army or temporarily expanding law enforcement powers to recover from a disaster or to prevent a pandemic does not raise concerns about the restriction of constitutional rights, mainly because of the unquestioned uniqueness of the situation. Promoting the infringement of fundamental rights and the sidestepping of the rule of law 'for the greater good,' because of 'national security,' or to fight the 'war on terror' is a wholly dissimilar matter. Nor is this a novel debate, as 'national security' has always been the magic spell to justify a wide range of political decisions.

A good example is when in 1960 the Kennedy administration tapped the telephone of Martin Luther King 'in the days when the attorney general could authorize a national security wiretap without a warrant.'[64] Similarly, in 1970 and 1972 the Nixon administration engaged in wiretapping, claiming the very same 'national security' excuse in an investigation against the Jewish Defense League.

> In 1972, however, the Supreme Court had rebuked the Nixon administration by holding, in a case involving Students for a Democratic Society, that the prior approval of a neutral judge … was required in all cases involving domestic organisations.[65]

This did not prevent subsequent administrations (not only in the US, as the *Echelon*, *Prism*, and other high-tech scandals revealed over time) from continuing to operate secret surveillance programmes and other activities hidden under the typical 'national security' carpet. It is clear that, in this conceptual framework, public policy and the rule of law are no longer equal weights on the scales.

This administrative drift is best explained by identifying the four stages of a strategic analysis process. Firstly there is the political stage, setting the specific goal. Secondly, there arises the strategic stage that determines the appropriate methodology to be used. Thirdly, there is the operative stage, where the wheels are set in motion. Fourthly, there is the tactical stage, when the objective is achieved by way of a specific action.[66] If the rule of law is purely a political principle, it directly constrains the will of the powers-that-be. If, on the other hand, it is merely a strategic or pragmatic instrument, it is reduced to a component of political will.

64 Dershowitz 2003: 159
65 Dershowitz 1983: 39.
66 Disma 2019.

The judicial function

Is this phenomenon to be explained by some dystopian *realpolitik* based on the growing global appeal for relativism? Is it simply an application of the infamous mantra that 'might is right'?[67] This disheartening possibility does not necessarily lead ineluctably to the conclusion that the task of the rule of law in limiting the authoritarian use of power has been extinguished. Looking at the function of law and rights as part of the architecture of public policy, but subjected to the rule of law, it is possible to recognise their role as a counterbalance to the exercise of political will, rather than one of the many policies that must serve the interests of the State.

In practice, this means that courts play an active role in shaping, and sometimes creating, a political goal. This important judicial dimension of the formation of public policy lies outside the scope of this book. Suffice it to say that courts do play a part in both the expression and implementation of the political goals of the State. The American Supreme Court is the most striking illustration.

There are several very recent instances of institutional conflict between the judiciary and executive.[68] One will suffice. The situation in Poland between 2019 and early 2020 is a case in point. PiS, Poland's ruling party, claimed that 'judges are self-serving, unelected elites who substitute their own preferences for those of voters.'[69] It therefore enacted strict limitations on the autonomy and independence of the courts. The legislation 'give[s] the government ever more control over the judiciary, violating the commitment to uphold the rule of law that Poland made when it joined the European Union.'[70]

In response, not only Poles but judicial officers from several EU countries marched in Warsaw to protest against this restriction on the courts' powers, and to reaffirm the importance of safeguarding the independence of the judiciary. This is a vivid illustration of the significance of the rule of law as a restraint on untrammelled executive power. The participation of foreign judges in opposing the Polish legislation is a reassuring manifestation of the importance of this principle. It is, however, worth asking whether these judges were objecting as concerned citizens or in their

67 Coined by Redbeard 1896.

68 The recent 'prorogation' judgement of the UK Supreme Court has been widely criticised on the ground that the judges, by ruling that the Prime Minister's decision to prorogue parliament was unlawful, were acting in a political rather than a judicial manner: *R (on the application of Miller) v The Prime Minister*; *Cherry and others v Advocate General for Scotland* [2019] UKSC 4. See Wacks 2019. On the general question of legislative constraints on judicial power, particularly in unjust societies, see Wacks 1984, 1998, 2009, 2021b.

69 'Poland's Ruling Party Should Stop Nobbling Judges.' *The Economist* 23 January 2020.

70 Ibid.

official capacity. If the latter is the case, under what authority were they acting? Is this an attempt to establish, outside the usual diplomatic channels, the *de facto* right of an international, unofficial gathering of judges to prescribe or question the agenda of a sovereign State? Leaving aside the merits of the protest, it is clear that civil society is no longer the only body to claim a role on the (international) political stage, and to upstage the traditional players.

Post-nationalism and the rule of law

The prospect of an international, integrated legal order does therefore appear, as Krisch contends, unlikely. Although, what he calls 'compromises with the rule of law ideals' may better be described as the forfeiture of individual rights. This captures more accurately the power relations between politics and rights, as it is more evident when rights have been suppressed, or when courts thwart or obstruct public policy goals. This is not a compromise, but an exercise of raw power: attainable, but not necessarily legal.

Preserving the rule of law as non-negotiable avoids the slide into expedient compromises by governments. It is preferable to defend the rule of law as a means of frustrating the denial or forfeiture of rights when they stand in the way of political goals. This is not merely a matter of semantics; it underlines the centrality of the protection of rights that is a fundamental element of the rule of law.

In contrast to Krisch's post-nationalist, compromise-based approach, a reinforcement of the rule of law principle at the *domestic* level could guarantee that those who exercise political power are always accountable for their public policy (as in 'political goals') and public policies (as in 'technical instruments to pursue political goals'). This ensures that where the State is sufficiently strong it ought to command compliance with the rule of law, rather than infringe it. This is a matter of the utmost importance for the understanding of the role of 'national security' (which we have yet to define; see below) especially because, as pointed out, the mere invocation of the term is supposed to cause all legal constraints to disappear.

In this regard, the experience of the Italian, French, and Nazi-German public security legal framework is a useful exemplar. The original Italian political design dates back to the end of the 19th century, under the liberal monarchic regime:

> In 1880 the public security services previously had an organized structure, and a political office was set up to deal with political and confidential matters … In the three years after 1880 other measures followed, such as … the organization of the service for the

surveillance of convicted offenders, with the creation of a biographical register of suspects.[71]

The fascist regime took a further step when on 14 January 1923 it issued Royal Decree n. 31,[72] that established a 'voluntary militia for national security' (*Milizia volontaria per la sicurezza nazionale*—MVSN), whose duty was to cooperate with armed and public security forces, i.e. the police, to protect public order. The aim was to detach the army from any political activity of the police that, in turn, fell under the authority of the Ministry of the Interior.[73] As a consequence the Ministry's powers were enforced by both the *Guardie di pubblica sicurezza* (whose task was to ensure the security and safety of daily life) and the MVSN (whose duty was to exercise political control over the citizen's political views).

The grip of executive power over citizens became tighter in 1931 with the Unified Collection of Public Security Laws (*Testo unico delle leggi di pubblica sicurezza*—TULPS),[74] that is still in force.

Complementing the role of the Milizia, the TULPS gave an almost free hand to the security police, in respect of direct power of control over citizens forced to provide evidence of their 'good social bearing' and moral standing. It also endowed the public security authority with the power to allow or forbid the running of specific businesses, and to authorise public gatherings and entertainment. These extensive powers were limited only by the possibility of invoking the intervention of the Ministry of the Interior, as no judicial review of the decisions or acts of the police was possible.

In its journey toward democracy, Italy maintained, and continues to maintain, the TULPS as an essential part of public order and security legislation. Over time, however, a series of amendments progressively dismantled its fascist-grounded architecture and redesigned it around a robust and court-based supervisory role. This is evidence (empirical, though evidence nonetheless) that the rule of law plays a central role in the shaping of public policy.

France took a similar approach to Italy, creating in 1934 the *Direction générale de la Sûreté nationale* as a political police force (thus, as a domestic body) lately renamed as *Police Nationale*. And so did Nazis in Germany

71 Tosatti 1997: 217.

72 Regio Decreto 14 gennaio 1923 n. 31 'con il quale viene istituita una milizia volontaria per la sicurezza nazionale' in Gazzetta Ufficiale del Regno d'Italia 20 gennaio 1923 n. 16 http://augusto.agid.gov.it/gazzette/index/download/id/1923016_PNC (visited on 20 January 2020).

73 Foderaro 1939.

74 Regio Decreto 18 giugno 1931 n. 773. 'Approvazione del testo unico delle leggi di pubblica sicurezza' in Gazzetta Ufficiale del Regno d'Italia 26 giugno 1931, n. 146 https://www.gazzettaufficiale.it/eli/id/1931/06/26/031U0773/sg (visited 19 January 2020).

that firstly in 1931 created the *Sicherheitsdienst* (a party—i.e. *private*—intelligence body) and later, between 1934 and 1936, regrouped together in a global infrastructure of police control, the *Geheime Staatspolizei* (Secret Political Police) and the *Kriminalpolizei* (Criminal Police) under the *Sicherheitspolizei* (Security Police), and finally, in 1939, everything under the *Reichssicherheitshauptamt* (Central Office of Reich Security).[75]

Is 'national security' a legal concept?

It is interesting to note that the very same 'threat,' i.e. political activism, was characterised by the fascist, French, and Nazi legislations as a '*national security*' issue, and by the UK's Public Order Act issued during the same period[76] as a '*public order*' concern. But were these two concepts interchangeable? And, most importantly, are they so regarded today?

Legal categories and domestic legal tradition are deeply connected; hence there is not a necessary equivalence between the meanings of the same terms in different legal systems. Nevertheless, in the case of 'public order' these distinctions are negligible as throughout Europe there was, and currently is, a general acceptance that this concept is related to maintaining (and, in certain cases, restoring) the 'peace of the land' by enforcing the core social values of a given historical moment. In contrast to the concept of 'public order' which, as shown above, has full citizenship status in legal and constitutional theory, 'national security' does not.

Apart, perhaps, from French and Mussolini's legislations that used the phrase to denote political activism as a national security matter, the latter was born and developed in the field of political science rather than in the domain of jurisprudence:

> [W]hen political formulas such as 'national interest' or 'national security' gain popularity they need to be scrutinized with particular care. They may not mean the same thing to different people. They may not have any precise meaning at all. Thus, while appearing to offer guidance and a basis for broad consensus they may be permitting everyone to label whatever policy he favors with an attractive and possibly deceptive name.[77]

A 2013 study by the Council of Europe and the European Court of Human Rights entitled *National Security and European Case Law* admits:

75 For an account of the Nazi security apparatus, see Gellately 1991: 23–38.

76 The Italian decree was issued in 1931; the UK statute (discussed in Chapter 1) was passed in 1936.

77 Wolfers 1952: 481.

> National security is mentioned in paragraph 2 of Articles 8, 10 and 11 of the European Convention on Human Rights (ECHR) as the first of the 'legitimate aims' making it necessary to restrict these rights. The term is not clearly defined, however, and could even be said to be somewhat vague. The European Commission of Human Rights … considered moreover that it could not be comprehensively defined, thus giving it a degree of elasticity and hence flexibility, which is reflected by the margin of appreciation which states have in this sphere. Although its limits are difficult to define, European case-law has made it possible to assign some substance to the concept of national security … It most definitely includes the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incitement to breach military discipline.
>
> (CoE, ECHR 2013)[78]

While 'national security' remains outside of the ambit of the system of legal rights, it makes little sense to try to connect the two ends of a bridge that are on different levels. From a public policy perspective this may be a viable option, as it allows the powers-that-be to retain maximum operational options. But the essential, inescapable need to harmonise political decisions with the rule of law indicates the importance of achieving—if possible—a normative definition of national security as the only meaningful way to identify *quis custodies ipsos custodies*, or, at least, to find some way to link political objectives with legal principles.

In this regard, there is support from the manner in which two of the most prominent security agencies—the British Government Communication Headquarters (GCHQ) and the US National Security Agency (NSA)—are regulated. According to the British Intelligence Service Act of 1994, the GCHQ may use its resources:

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
(c) in support of the prevention or detection of serious crime.[79]

78 Council of Europe (2013) *National Security and European Case-Law* p. 4 https://rm.coe.int/168067d214 (visited 22 December 2020).

79 Intelligence Services Act of 1994, Chapter 13, Article 3.

Although the Act does not provide a clear indication of what constitutes 'national security,' it expresses what national security is *not*: it is neither related to the economic well-being of the UK nor to its public security/safety. The text of the statute suggests that national security is connected with *government* policy rather than with the protection of the kingdom itself, and that it is a *meta-concept* including more clearly defined concepts such as defence and economic well-being.

This conclusion is reinforced by an analysis of the Terrorism and Border Security Act of 2019 that:

- Updates terrorism offences for the digital age, and to reflect contemporary patterns of radicalisation.
- Disrupts terrorism by enabling the police to intervene at an earlier stage in investigations.
- Ensures that sentences properly reflect the seriousness of terrorism offences, and strengthen the ability of the police to manage terrorist offenders after their release.
- Strengthens the country's defences at the border against hostile state activity.[80]

Again the law does not mention a specific legal category of 'national security'; instead it amends provisions based upon a traditional and well-established framework.

A similar conclusion is reached from the analysis of the US national security apparatus which continues, in the main, to be based on the National Security Act of 1947, amended in 1949. The various doctrinal attempts to define national security tend to oscillate between mimicking the notion of 'public order' to that of 'public security.' Or they lean toward the military dimension of the concept by embracing the role of war as one of the instruments with which to protect national interest.

> The articulation of national interests, objectives, policies, and commitments linked to use of the instruments of national power is sometimes referred to as 'grand strategy,' 'grand national strategy,' or, currently in the United States, 'national security strategy.' Grand strategies or national security strategies are implemented by subordinate strategies—political or diplomatic strategies, economic

80 United Kingdom Home Office 'Counter-Terrorism and Border Security Act 2019 Overarching Fact Sheet,' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778175/2019-02-12_Overarching_Fact_Sheet_RA.pdf (visited on 30 January 2020).

> strategies, national military strategies, and so forth—for the use of each of the instruments of national power.[81]

As useful as they are for a political scientist, none of these approaches offer a *legal* definition of national security. And this becomes apparent when one reads the National Security Agency's regulatory framework:

> The U.S. Constitution, federal law, executive order, and regulations of the Executive Branch govern NSA's activities. As a Defense Agency, NSA operates under the authority of the Department of Defense. As a member of the Intelligence Community, NSA also operates under the Office of the Director of National Intelligence. NSA/CSS activities are subject to strict scrutiny and oversight both from outside and from within. External bodies such as the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI), the President's Intelligence Oversight Board, the Foreign Intelligence Surveillance Court, the Department of Defense, the Office of the Director of National Intelligence, and the Department of Justice help ensure that NSA adheres to U.S. laws and regulations that are applicable to the Agency's activities.[82]

The NSA is a multi-faced and cross-departmental entity; it neither operates nor is it monitored by a distinct branch of government. Furthermore, it functions under congressional oversight. Apart from its name, however, nothing in its powers or the chain of command hints at a unique, legal definition of national security.

Thus, to answer the question posed above, it appears that, first, assigning national security legal status is unattainable because of its intrinsic and prevailing political nature that does not fit well with the rigidity of a normative definition.

Secondly, and as a consequence, national security is not, nor should it be, a goal or a concept in itself, but rather the result of the coordinated contribution of public policy governing different sectors of the security apparatus: police operations (public security), court rulings (judicial action), border defence (military control)—each individually subject to the rule of law.

Rapid changes in the contemporary geopolitical scenario have led to an increasing inclusion of national security *into* the body of laws. In other words, while the rule of law develops into a *political* concept, national

81 US Marine Corps 1997. 'Strategy.' MCDP 1-1 PCN 142 000007 00. Washington DC. p. 39.
82 'National Security Agency Oversight FAQs,' https://www.nsa.gov/about/faqs/oversight-faqs / (visited 30 January 2020).

security moves in the opposite direction towards a *legal* concept. This is because of the need to place national security firmly in the hands of the executive because of the weaponisation of rights or, as some scholars calls it, 'lawfare.'[83]

Other legislation on export controls, consumer protection, and international trade agreements can equally be weaponised without explicit parliamentary oversight. As mentioned, it is enough to claim that a certain country is involved in human rights violations or unfair commercial practices to justify the imposition of embargoes or special customs duties. It does not matter whether these allegations relate to a Far Eastern country exploiting child labour, or a Western multinational infringing the right to privacy of a European citizen. In the above cases, national security remains the political goal to be achieved by lawfare. But when national security itself represents the core of the lawfare attack, it must necessarily be embedded into a legal provision. China is strengthening its legal arsenal with legislation relating to the export of dual-use goods, cybersecurity, and personal data protection that, mirroring the Western attitude, reaches well beyond national borders. They are weaponised by design.[84]

The direct consequence of national security becoming a legal category is its submission to the rule of law. It is, therefore, not surprising that the inescapability of the legislative gateway is not welcomed by Western governments. Having accepted the necessity of specific legislation, as the Iranian example clearly shows, they lobbied to render it as muddy or vague as possible.

In 2007, the Italian parliament redesigned from scratch the legal framework of the intelligence sector. According to Article 1 of Law 124 of 2007, the President of the Ministers' Council is solely responsible for the choices regarding the 'policing of information for the security, in the interest and for the defence of the Republic and the democratic institutions.' The original architecture of this law is established on the traditional paradigm of spy-based intelligence and of the necessity to shield its activities from the curious gaze of the 'non-expert' (whether they be magistrates, journalists, or concerned citizens). It is not by chance that the legislation in question is concerned with regulating State secrets, immunity from prosecution of the operators, and the possibility of accessing databases, all from the perspective of rendering the activity of information gathering more efficient.

A Gordian knot fashioned from an intricate tangle of laws, decrees, and ministerial orders expressed in an obscure and bureaucratic legalese transformed the very nature of the matter. Firstly, the Council Presidency now takes an active role not only in defining policies on information gathering

83 Dunlap 2015: 823–838.
84 Monti 2020b.

for security, but also in the protection of the physical and logical infrastructures of the nation. Secondly, the presidency has expanded its reach from security *tout-court* to the protection of national interests. As a consequence, it has increased its power beyond the traditional information-gathering domain. It now possesses the ability to intervene directly in every economic operation deemed contrary to Italian interests. Moreover, the presidency is given an 'Internet Kill Switch'—the power to shut down the entire national telecommunications network—as well as the power of controlling critical Italian infrastructure.

National security and the rule of law—again

The most important outcome of the 'normativisation' process of national security—and, thus, its compliance with the rule of law—is that, as a legal category, it is subjected to direct judicial oversight. The process is still in its early stages, but it can hardly be disputed that national security cannot remain hidden in the grey zones of 'principles.' It is essential that it becomes transparent, and takes its place in the arena of competing rights. Likewise, the more national security is designed as a provision rather than as a principle, the clearer is the responsibility of the executive when it stamps the moniker 'Official Secret' on certain matters.

The practicality and reasonableness of this approach are evident in view, on the one hand, of the fact that governments are entitled to a free hand in determining their political agenda, but, on the other, that they must be subject to a watchdog that ensures that freedom is not abused. Even though the concept of national security may continue to defy clear definition, its key components do not. By asserting the inescapability of the rule of law in respect of police, judicial, and military powers to protect the public against attacks on national security, the abuse of such powers may be checked.[85]

An actual instance of this tension has arisen in the form of the differences between a group of EU member States, on the one hand, and the European Court of Justice, on the other, regarding the extent to which fundamental rights should be sacrificed on the altar of the fight against crime and terrorism. France, Belgium, and the UK raised concerns about the restrictive approach adopted by the European Court of Justice in regard to carpet-retention of telecommunications traffic data imposed on electronic communication service providers. The court declared invalid the EU Directive

85 An indirect acknowledgement of the sustainability of this conclusion comes from the EU Advocate General's Opinions in Case C-623/17, Cases C-511/18, C-512/18, and Case C-520/18. Court of Justice of the European Union. Press release 4/20, Luxembourg, 15 January 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf (visited 30 January 2020).

2006/24/CE because of its excessive interference in the right to respect for private and family life, as well as in the right to the protection of personal data. The decision has been criticised on the ground that it will impair the ability of a State to safeguard national security and fight crime and terrorism.[86]

Rejecting these concerns, the EU's attorney general declared:

> [T]he fight against terrorism must not be considered solely in terms of practical effectiveness, but in terms of legal effectiveness, so that its means and methods should be compatible with the requirements of the rule of law, under which power and strength are subject to the limits of the law and, in particular, to a legal order that finds in the defence of fundamental rights the reason and purpose of its existence.

While this statement of principle sounds robust, it is actually evidence of the difficulty in applying the rule of law to constrain the will of those who exercise political authority. This is because the attorney general then refers to:

> [T]he retention of specific categories of data that are absolutely essential for the effective prevention and control of crime and the safeguarding of national security for a determinate period adapted to each particular category.

Moreover, he adds:

> [T]here is no reason why, in exceptional situations characterised by an imminent threat or an extraordinary risk warranting the official declaration of a state of emergency, national legislation should not make provision, for a limited period, for the possibility of imposing an obligation to retain data that is as extensive and general as is deemed necessary.

In other words, as soon as a sovereign State declares a state of emergency, the check-and-balance mechanism is rendered nugatory or, at least, less effective. This is perfectly reasonable in theory but does not easily translate into practice.

86 Joined Cases C-293/12 *Digital Rights Ireland and Others* and C-594/12 *Seitlinger and Others*, in which the Court declared the invalidity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54). Court of Justice of the European Union. Press Release 4/20, op. cit.

Indeed, when we are pummelled almost daily by news about 'rogue countries' threats,' 'the war on terror,' and 'international crime syndicates' takeovers' it is easy to succumb to the political claims about the urgency of emergency or exceptional legislation to cope with 'unprecedented and unforeseeable events.' And if words maketh (political) truth, then propaganda (or, in more fashionable terms, 'consent manufacturing' or 'information control') is an inescapable necessary tool by which to bypass or weaken the efficacy of legislative oversight.[87]

Decision 797 of the EU Council 'establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States'[88] and declares that

> targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State.[89]

Restrictive measures include freezing financial resources and, under Article 4, taking

> the measures necessary to prevent the entry into, or transit through, their territories of:
>
> (a) natural persons who are responsible for cyber-attacks or attempted cyber-attacks;
> (b) natural persons who provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;
> (c) natural persons associated with the persons covered by points (a) and (b).

87 The Council of the European Union Decision (CFSP) 2019/797 of 17 May 2019 is a practical example of how political goals can overcome the rule of law by way of formally valid, but essentially empty, legislation. See Council of the European Union 'Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,' https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797&from=GA (visited 30 January 2020).

88 Recital (7).

89 Recital (9).

Instead of using the unquestionable political power of declaring an individual *persona non grata*, without the need to provide a motive for the decision, the EU chose the option of enforcing an indictment without trial. So, under Decision 797 a non-EU citizen can have his property, assets, freedom of movement, and the right to a fair trial denied before his responsibility for acts regarded as criminal offences throughout the Union and abroad are judicially declared as such. And the same fate awaits whoever is 'associated'[90] with the person 'responsible' for these acts. In other words, the need for national security is achieved by purporting to respect the rule (and the role) of law, while actually negating it.

National security as control over information

Summing up, it seems reasonable to conclude, firstly, that the connotations of national security, in the political domain, are too diverse and imprecise to provide adequate legal clarity, especially when the concept is deployed across disparate jurisdictions with dissimilar political, social, and legal cultures. The search for a satisfactory legal notion of national security is unlikely to succeed. Therefore, secondly—and at least until international agreement on its legal definition is reached—it will continue to operate as a meta-concept which entails the balancing of the often-divergent legal principles that are already well established in the domestic and international sphere.

Nonetheless, a legal definition of national security is essential to turn a political goal into something that can be matched (and balanced) against other public responsibilities and fundamental rights.

When attempting a taxonomy of State powers in the previous chapter, we suggested that 'public security' is what keeps the citizen safe, 'public order' is what keeps citizens quiet, and 'border defence' is what protects the country from foreign invasion. What is plainly missing in the legal domain is something that protects—and permits the enforcement of—the 'national interest,' i.e. the *acquis* of economic, political, cultural, and social goals of the State as carried out by the government. By stipulating that the connection with the past can be severed, a new legal definition of national security might be precisely this: *the duty (duty, not power) of the State to protect and enforce the national interest according to the rule of law*.[91]

But how does this definition of national security differentiate it from the other powers already in place? Firstly, national security works at a very

90 The word used in Para 4 of the Decision.

91 The extent to which the decline of the nation state has undermined the rule of law in European countries is among the themes pursued by Hannah Arendt who argues, inter alia, that this occurs when authoritarian regimes supplant democratic constitutional states. See Arendt 1958. For an outstanding analysis of the place of the law in Arendt's philosophy, see Volk 2015.

early stage of the State's protection system because it is, or ought to be, largely concerned with information gathering of any kind (not confined to 'military' or 'crime-related' data). Secondly, and consequently, it buttresses, or ought to buttress, other elements of the security apparatus by the analysis, selection, and provision to the appropriate authorities of information. And thirdly, it acts as a gateway between the *raison d'État* and the rule of law by injecting into the system bits of information to be processed according to the law of the land.

Decision 797, the concerns expressed by EU members about the European Court of Justice's crackdown on disproportionate State-manned mass surveillance, the duties of GCHQ and the NSA, and the involvement of the private sector in law enforcement and intelligence services activities all have this in common: the centrality of information as a fundamental feature and starting point of the (national) security process. This is the subject of the following chapter.

3

PUBLIC POLICY, NATIONAL SECURITY, AND INFORMATION

In Chapter 2 we defined national security as control over information that may facilitate the transition from the political to the legal. The need to accord national security independent legal status arises from the observation that traditional categories such as 'law and order' and 'military defence' extend to the many fields associated with national security. However, if national security must retain its Janus' face—political and legal—we require a clearer statement of its position among existing concepts. This may be achieved by recognising its important relationship with information. As opposed to conventional information gathering by law enforcement and military authorities, the executive ought to manage a broader spectrum of data to facilitate political decision-making. This would include the collection, analysis, and protection of all the information relevant to the survival of the State.

This method is already adopted in the less traditional domains of the economy, industry, finance, science, and social sciences, to name only a few. As a practical matter, these activities can be undertaken using so-called 'open source intelligence,' by technological means such as eavesdropping and other forms of technology-based intelligence, and covertly using informers and spies.

It is not hard to recognise in this abstract description the structure of the intelligence services of more advanced countries. In democratic systems there is a clear distinction between information-gathering in the interests of the executive and the same activity carried out by law enforcement authorities for crime prevention and control.

But the law normally imposes limits on the exercise of these powers. In some cases, for example Italy, intelligence operatives are prohibited by Law 124 of 2007 from endangering or taking a life in a non-war situation, although they can commit non- serious crimes when on duty[1] and act as

1 However, that did not prevent Italian intelligence agencies from allegedly being involved—if not actively taking taken part—in the *Strategia della tensione*, a series of terrorist actions culminating in 1969 with the bombing of Piazza Fontana, that ignited the *Anni di piombo*

DOI: 10.4324/9780367809775-3

intermediaries in cases of kidnapping[2] and other politically sensitive crimes. Countries inevitably differ in their attitude toward this matter. Some condone—if not actually support—human rights infringements and violence even in non-war settings. Others, notably the US and UK, bury these powers in a deep stratum of foggy legislation, internal directives, and 'legal opinions.' Arab countries and Israel, as well as Russia and certain Indo-Pacific States, do not pretend that they do not sanction such methods.

In 1975 the *Interim Report* of the US Senate, better known as the *Church Committee*,[3] investigated allegations that the US actively plotted targeted assassinations against individuals known to threaten American interests, including Fidel Castro.

The Church Committee's report is a remarkable document on national security (or more appropriately, 'national *policy*'). At its core is the principle that 'the truth about the assassination allegations should be told because democracy depends upon a well informed electorate.'[4] This sounds more like a public relations damage control technique rather than a genuine commitment to the truth. Conveniently, at the time of the investigation those who could shed light on the topic were long dead or old enough to have faded memories of the facts. However, two crucial issues emerge for the purpose of this book. Firstly, the *principle* of the right to know about such a sensitive matter is strongly affirmed. Secondly, the wide enforcement of 'plausible deniability' has been the standard operating procedure to keep, at least formally, the president unaware of what the intelligence agencies were plotting.

What is pertinent to the present discussion is the relationship between rights, the law, and policy as elucidated by the committee. The US lacked a single piece of legislation that referred to targeted killing as a foreign policy tool or as a feature of intelligence operations. However, according to the report, the National Security Act of 1947 created the National Security Council with the power to direct the CIA in national security matters. The National Security Council 'issued a top secret directive granting the CIA authority to conduct covert operations.'[5] Covert operations included

(Years of Bullets). Despite several trials, it has not been possible to reach a definitive conclusion because the government invoked State secret protection, thus preventing the prosecutors from investigating the matter thoroughly, including the relationship with CIA involvement. See Dondi 2015.

2 RAI TG2 Post 7 January 2021—statement of former Italian president of the ministers' council Matteo Renzi, https://shar.es/aohU97 minute 24,41 (visited 10 January 2021).

3 US Senate of the 94th Congress (1975) *An Interim Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities* Washington, US Government Printing Office, https://www.intelligence.senate.gov/sites/default/files/94465.pdf (visited 4 January 2021). Hereafter the 'Church Report'.

4 Church Report: 2.

5 Ibid: 8.

propaganda, economic warfare, political action, sabotage, demolition, and assistance to resistance movements and 'all activities compatible with the directive.' Moreover, according to the memorandum of the CIA's General Counsel quoted in the report, covert operations had to obtain the necessary policy approval before being deployed. Finally, it was up to CIA officials to decide whether targeted killing required such approval, and if the approval could be taken for granted or presumed as existent.[6]

As in the boiling frog metaphor, where the slow rise in the water temperature does not allow the poor creature to understand what is going to happen until is too late, the multiple layers of regulations and directives were fashioned so that from the high level of statute not mentioning homicide as a policy tool, through the vague terrain of administrative decisions, down to a non-binding legal opinion, CIA officers were, in effect, granted an almost free hand. This is a striking example of how politics interact with legislation and rights, preserving the facade of the rule of law while actually departing from it.

What happened after the publication of the Church Committee is more revealing of this attitude. In the year of the report's publication, President Gerald Ford issued Executive Order 11905 that formally banned targeted killing. That did not, however, end the 'active' role of the CIA in the Middle East and the practice of drone-operated targeted killing, once again thanks to an exercise in legal interpretation. Moreover, contrary to the Church Report's bold statement about the right to know, post-9/11 US administrations fell back on an obfuscation strategy based on the justification of 'national security' and generalised rhetoric that 'we are at war.'

The Bush administration relied heavily on targeted assassinations and pre-emptive strikes against members of al-Qaeda, as later essentially did President Obama while claiming that these actions conformed to the rule of law:

> The Obama administration has sought to portray itself as acting in accordance with the rule of law, as a contrast to the George W. Bush administration's reshaping of legal parameters. Importantly the Obama administration, seeking to portray itself as an ethical alternative to the Bush administration, not only continued to use targeted killings, but also vastly increased their use against al-Qaeda and affiliates.[7]

6 Ibid.
7 McDonald 2017: 2.

In particular, 'the Obama administration's defence of targeted killings hinges on the idea that the United States is at war with al-Qaeda, and that targeted killings represent a necessary act in the context of this conflict.'[8]

It is outside the scope of this book to consider the extent to which the US approach to targeted killings and its implications in respect of States' sovereignty and fundamental rights have legal merit. What matters is the attempt to balance the executive's claimed desire to 'do the right thing,' on the one hand, and the legislature's duty to preserve democratic constitutional values, on the other.

A similar conflict arises between the government and parliament in the UK in relation to assassinations and violating the sovereignty of foreign countries as an acceptable option in pursuit of protecting national security interests.

According to Section 7 of the UK Intelligence Service Act of 1994:

> If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.[9]

Contrary to the Italian legislation, this provision does not limit the kind of crimes that might be committed in mainland Europe or elsewhere. It does not authorise killing or other human rights infringements such as 'enhanced interrogation techniques,' but it does not forbid them either. And to be on the safe side, Parliament is currently debating a government bill to amend the Regulation of Investigatory Powers Act 2000 (RIPA) to authorise criminal conduct of covert human intelligence. It is noteworthy that this bill (not yet passed at the time of writing) requires a 'criminal conduct authorisation' before the act is committed. According to the fourth paragraph of the new Section 29B to be inserted in RIPA:

> A person may not grant a criminal conduct authorisation unless the person believes … (b) that the authorised conduct is proportionate to what is sought to be achieved by that conduct.

Moreover, the next paragraph clarifies that

8 Ibid: 67.

9 Intelligence Service Act of 1994, https://www.legislation.gov.uk/ukpga/1994/13/section/7 (visited 4 January 2021).

> A criminal conduct authorisation is necessary on grounds falling within this subsection if it is necessary—(a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; or (c) in the interests of the economic well-being of the United Kingdom.[10]

In other words, those who grant the criminal conduct authorisation must *believe* that such authorisation is necessary. And the authorisation includes, without any differentiation, national security (intelligence, but also military), crime prevention and public order management (law enforcement and police forces, civil services such as revenue services), and a vague notion of UK 'well-being' (various government departments and agencies).

There is, at least in theory, a distinction between the approaches of the UK and US:

> British intelligence and security agencies have had to ensure that any substantive involvement in prisoner abuse takes place in ways that maintain a level of procedural adherence to human rights norms and legal commitments, thus enabling ministers to routinely proclaim the continued and unwavering prioritisation of human rights in the fight against terror. This approach has been markedly different from that of the US, which suspended core commitments under international law and developed specific politico-legal justifications for the indefinite detention and torture of 'terror suspects'.[11]

Two Italian cases, that gained international media exposure, elucidate the questionable role of the 'national security' claim as a shortcut to pursuing (geo)political goals arising from intelligence operations carried out on Western soil rather than in distant parts of the world. The first is the kidnapping in Milan in 2003 of the mullah Abu Omar organised by the CIA that led to the indictment of 23 US intelligence operatives,[12] three of whom were later pardoned by Presidents Napolitano and Mattarella.[13] The second, in 2013, was the expulsion from Italy of Alma Shalabayeva, wife of a Kazakh dissident wanted by the authorities in his country.[14] The expulsion was

10 UK Parliament *Covert Human Intelligence Sources (Criminal Conduct) Bill 2019–21*, https://services.parliament.uk/bills/2019-21/coverthumanintelligencesourcescriminalconduct.html (visited 7 January 2021).

11 Blakeley and Raphael 2017.

12 Donadio 2021.

13 *La Stampa* online edition *Abu Omar, il sequestro, le condanne e la grazia: 16 anni di misteri* 31 October 2019, https://www.lastampa.it/esteri/2019/10/31/news/abu-omar-il-sequestro-le-condanne-e-la-grazia-16-anni-di-misteri-1.37814463 (visited 9 January 2021).

14 Giglio 2020.

speedily executed and—according to the first instance ruling of 14 October 2020 by the court of Perugia—was unlawful, and resulted in the conviction of two *Polizia di Stato* officers for kidnapping and false statements in official documents.

Of the two, strictly speaking, only the Abu Omar case falls within the definition of 'extraordinary rendition' as a tool of counterterrorism. Instead, the Shalabayeva case is technically part of 'normal' activity to combat illegal immigration, since the handing over of the woman to the Kazakh authorities was the logical and legal consequence of an expulsion order issued by a (lower) court.

However, details revealed by the press at the time[15] and which emerged during the trial[16] tell a different story whose substance is not dissimilar to the Abu Omar case. It seems that international relations played a significant role. The procedure would almost certainly have been as follows. Initial contact between the head of the cabinet of the Minister of Home Affairs and Kazakh diplomats who would have asked for support for the arrest of a wanted man (but who styled himself a political dissident) located in Rome. The Italian authorities were unable to locate him and therefore 'switched back' to his wife. The police held her in violation of the immigration law and handed her over to the Kazakh authorities after an expulsion procedure that the court in Perugia, as mentioned, found to be unlawful. The evidence during the trial of the police officers raises a number of questions, but the fundamental issue is the fact that, unlike the Abu Omar case where four governments imposed restrictions based on State secrecy,[17] in the Shalabayeva case they did not.

We may never discover what happened in the 'preliminary phases' of the Shalabayeva operation and, in particular, in the early contacts between the Kazakh and Italian institutions. But the non-imposition of State secrecy suggests that in this case we are not faced with actions carried out in the name of the special interests of the Republic. Therefore, closing the circle, if it is true that the aim of the Shalabayeva affair was taking hostages[18] and

15 *La Stampa* online edition 'Caso Shalabayeva, le tappe della vicenda' 26 June 2019, https://www.lastampa.it/cronaca/2015/11/26/news/caso-shalabayeva-le-tappe-della-vicenda-1.35210496 (visited 9 January 2021).

16 *Radio Radicale* (2019–2020) audio recording of the criminal trial hearings for the alleged abduction of Shalabayeva, https://www.radioradicale.it/processi/1317/processo-renato-cortese-ed-altri-presunto-rapimento-shalabayeva (visited 9 January 2021).

17 *La Repubblica* online edition 'Abu Omar, governo conferma segreto di Stato.' 28 January 2013, https://www.repubblica.it/politica/2013/01/28/news/abu_omar_governo_conferma_segreto_di_stato-51441270/ (visited 9 January 2021).

18 Report *L'ostaggio* 25 November 2013, https://www.raiplay.it/video/2013/11/Report-del-25112013-3b2061ff-643d-4599-a1c6-65f6d01f8496.html (visited 9 January 2021).

not apprehending a criminal, we can certainly regard it as an extraordinary rendition even if it was not treated as such by the Italian government.

However, the fact that it could have happened, and in the manner described by the media and which emerged during the trial, poses serious questions about the extent to which one can invoke a State's reasons to justify particular activities. And, above all, one should enquire whether the time has come to regulate this grey area of institutional activities carried out in the ostensible interests of a State. Otherwise we shall continue to hear the slogan 'in the name of national security' to defend abuses that damage not only the victims but also the trust of citizens in democratic institutions.

By contrast, authoritarian regimes do not—and do not need to—embark on intricate endeavours of legal design or disinformation. Nor do they need to draw a clear distinction between the realm of information-gathering and the exploitation of the results. The chief aim of their intelligence services is to protect the survival of the State by gathering information and taking active measures against those perceived as a danger. In other words, there is no distinction between *collecting* information and *using* it as a crude method by which to retain power.

In the recent past, among the 'usual suspects' are the infamous fascist secret police, *Ovra*, the Leninist *Čeka*, the German *Gestapo*, and McCarthyism in the US. However, the same methods have been deployed by Eastern countries during the Cold War and by South American dictatorships such as the notorious Argentinian government in the 1970s.[19]

The murder of Russian dissidents at home and abroad strongly implicates the government, although there is, as yet, no overwhelming proof that it is to blame. In the Arab world, however, the evidence is fairly persuasive:

> All Arab states rely on elaborate—often redundant—security establishments for regime security. The leaderships of states as politically diverse as Morocco, Egypt, Syria and Saudi Arabia charge their intelligence agencies with the mission of neutralising an array of threats from ruling establishment conspiracies to terrorist groups and foreign espionage … But the Arab secret services do more than collect and analyze information. In most cases, they are the sharp end of the spear, symbols of a state's power to coerce its citizens and intimidate its enemies.[20]

19 National Security Archive, *Inside Argentina's Killing Machine: U.S. Intelligence Documents Record Gruesome Human Rights Crimes of 1976–1983*, George Washington University, 30 May 2019, https://nsarchive.gwu.edu/briefing-book/southern-cone/2019-05-30/inside-argentinas-killing-machine-us-intelligence-documents-record-gruesome-human-rights-crimes-1976 (visited 7 January 2021).

20 Sirrs 2011: xx.

Two recent examples are paradigmatic of the Gordian knots enthralling the Arab approach toward intelligence, crime prevention, and national security. First is the assassination in 2016 of the Italian Cambridge graduate, Giulio Regeni, allegedly committed, according to Rome's public prosecutor, by Egyptian national security operatives.[21] The second is the killing in 2018 of the Saudi dissident Jamal Khashoggi at the hands of Saudi intelligence officers.[22]

British, American, and—in general—Western intelligence agencies are heavily regulated and subjected to parliamentary oversight. China and Russia have a legislative framework to manage national security and, at least apparently, provide citizens with legal protection. Even regimes that prioritise the rulers' security over the rule of law have to apply, at least to satisfy the international community, some form of legal control over the national security apparatus. Yet they all venerate the obscurity and vagueness of the legal categories which obscure the environment and foster the longstanding rule of the trade known as 'the Eleventh Commandment': *thou shalt not get caught*.

Secrecy is, of course, a critical component of information-gathering-based national security, but it can become either a buzzword or a shortcut to conceal less-than-noble activities. This is why national security warrants a distinct place in the legal taxonomy. It has two effects. Firstly, it elucidates the executive's relationship with other competing institutions. Secondly, it helps to create a balance with other democratic rights, in particular with the right to transparency and the right to privacy. There is, though, a paradox in legislation that rests on a historical (and anthropological) observation: that the untrammelled exercise of violence to preserve power existed long before the acknowledgement of the rule of law and human rights by several modern societies. The Bible admonishes the faithful not to seek vengeance on Earth as it belongs to God (or, in some cases, to His human representatives). However, the Torah teaches that 'should somebody come to kill you, thou shall stand against him and kill him first.' In these competing precepts lies the core of the problem. To ignore this is to fail to understand the eternal debate conducted by *machtpolitik* scholars and jurists.

The pursuit of self-interest, be it by an ancient ruler or a Westphalian sovereign State, has one fundamental limitation: the extent to which it can rely on the 'weight' of this interest so that other actors must give it due consideration. As the intricate relationship between the US and China shows,

21 Cruciati, Chiara, 'Verità per Giulio Regeni: a processo il regime e i suoi aguzzini.' *Il Manifesto* online edition 11 December 2021, https://ilmanifesto.it/verita-per-giulio-regeni-a-processo-il-regime-e-i-suoi-aguzzini/ (visited 8 January 2021).

22 *BBC News*, 'Jamal Khashoggi: All You Need to Know about Saudi Journalist's Death' 2 July 2020, https://www.bbc.com/news/world-europe-45812399 (visited 9 January 2021).

military might is no longer the weapon of choice to achieve these results. Economic, legal, and social warfare—as well as 'soft' attacks on computer infrastructure—are the preferred means of attack. In a word, it is *knowledge*, rather than simply information, that matters.

Power and secrecy

'Information is the new oil,' 'information is the new gold,' and 'knowledge is power' are three clichés that have found their way from the marketing claims of computer programme and hardware manufacturers to journalists, economists, sociologists, philosophers, and legal scholars. The analogy mistakenly accentuates the raw material rather than the actual knowledge necessary to make use of it. Oil was here for millennia before somebody devised a way to find, extract, and refine it on an industrial scale. Moreover, with the end of the Bretton Woods agreement and the rise of cryptocurrency, gold as a measure of value may relatively soon begin to decline.

From the dawn of time humans have sought to acquire and protect knowledge. It achieved a religious or mystical status. Today, however, knowledge has become a sort of spell that, once cast, causes things to happen. It has degenerated into an empty slogan or marketing tool. Its original, Hobbesian meaning—knowledge as something for the few,[23] whose ultimate goal is action[24]—has been entirely lost, at least in the *vulgata*.

In fact, knowledge and information are circularly connected. The former cannot exist without the latter, and vice versa. Information generates knowledge and knowledge assists in the discovery of new information or in understanding it in different ways. In the making of artificial 'intelligence' the purpose of accumulating a huge quantity of data is to feed it into a computer programme in order to gain (relatively) independent actionable knowledge.

It is the interaction between knowledge and information that operates to facilitate the exercise (and preservation) of power. There is, however, no point in acquiring information if one neglects the question of how it is to be used. Information may circulate freely if citizens are unaware of its meaning and, therefore, its value. It is no coincidence that in the intelligence cycle the gathering of information is flanked by its analysis.

If knowledge and information are pieces of gold, secrecy is the safe that protects them from theft, abuse, and loss. Moreover, if knowledge and

23 'Scientia potentia est, sed parva … Scientiae enim ea natura est, ut esse intelligi non possit, nisi ab illis qui sunt scientia praediti. Hobbes, Thomas Opera philosophica, quae latine scripsit, omnia in unum corpus nunc primum collecta studio et labore,' Molesworth 1839–1845: 69.

24 'The scope of all speculation is the performing of some action, or thing to be done,' Hobbes, Thomas, Ibid: 75.

information are power, secrecy is the engine that makes the cogs of power turn. More than knowledge and information, it is their *control* that accords rulers a strategical and tactical advantage over foes (and even friends). The Crypto AG scandal that will be addressed later in this book is but the latest iteration of the no-holds-barred attitude when national security is involved. 'Friend' or 'ally' status is not enough to prevent a State from gathering classified and confidential information from another friendly country.

Secrecy, in other words, is a core element of the exercise of power and rules the very foundation of a society, whether a tyranny, a democracy, or of many intermediate states between these two extremes. Whatever the political status of a regime, however, they all have one thing in common: the fact that control over information and knowledge comes with a tight grip on what, when, where, and how it is made public (or cannot be kept secret).

It is interesting to remark, in this regard, that there is no intrinsic difference between the role of secrecy under a dictatorship and under a democratic regime. As Orwell memorably demonstrated in *Nineteen Eighty-Four*, secrecy was instrumental to the sole preservation of power and citizens were entitled to know 'the Truth' only by way of the homonymous ministry, a cross between the fascist *Minculpop* (the Ministry of Popular Culture), the Nazi *Reichsministerium für Volksaufklärung und Propaganda*, and the Stalinist Главноеправление по охране государственных тайн в печати при СМ СССР (General Directorate for the Protection of State Secrets in the Press under the Council of Ministers of the USSR). The political stability of a country is attained—from Sparta to Pyongyang, by way of Washington DC and Beijing—by carefully preventing unwanted knowledge becoming freely available. Even the Vatican adopted a similar approach. As with all religions, it preserves its spiritual power by the creation of unfathomable mystery. The evidence usually provided to support this claim is Galileo's trial, often simplistically described as the attempt of the Vatican to safeguard its dogmas from the influence of science. However, 'new' disciplines and unconventional readings of the holy texts were not only a matter of heresy. They threatened also law, order, and public security, as the Cardinal of Venice wrote in 1843 supporting the establishment of the Holy Inquisition and justifying the participation of the civil authorities in the hunt for heretics:

> indeed, the popes erected this tribunal with no other goal than to investigate and punish … doctrines and actions whose goal is to subvert the foundation of the faith and trouble the peace of the land.25

25 Ancarani 1844: 6.

The not-so-covert operations to prevent 'rogue countries' from developing nuclear weapons by targeting facilities and scientists is but the most conspicuous and enduring example of the weaponisation of knowledge.

In the exercise of power there are no watertight domains. As the impact of the coronavirus pandemic dramatically demonstrates, when life-and-death decisions must be taken, pure knowledge mixes with science, and philosophy with politics.[26] Reliable and timely gathered information is also part of the decision-making process. But it cannot be achieved without secrecy as the go-between. At the same time, the spreading of targeted disinformation or uncontrolled fake news hindered the formulation and enforcement of a coordinated effort to stem the contagion.

In the past, the difference and relationship between knowledge and information were less clearly identified. Spartan military commanders secured their communications to their subordinates by wrapping a strip of fabric carrying written orders around a *scytale* of a specific size so that only those who owned an identical baton could properly re-wrap the strip and read the message. Julius Caesar adopted a similar method, employing a cypher system (later named after him) to exchange information with his generals.

However, secrecy was also a means by which to safeguard superior knowledge. It has been of paramount importance since the early days of civilisation. As pointed out, it attained a mythological status. The tale of Prometheus, the Titan who stole fire from the Olympians gods and gave it to mankind, is the archetype. However, the Pythagorean Hippasus of Metapontum and the Roman Republican jurist Gnaeus Flavius were real—as real as the consequences of their Prometheus-like actions.

The core of Pythagoras' philosophy was the idea that *everything is a number*. Around this core, Pythagoras and his followers built a comprehensive 'theory of everything' that accounted for the celestial planets moving through space. It explained also a 'public policy' aimed at maintaining order in society reflecting the mathematics-ruled universal order (through tyranny?[27]) and—as someone contended—the introduction of coinage.[28] The Pythagoreans' perfect harmony was disrupted by the discovery of numbers that cannot be expressed as a ratio—hence, irrational. Being aware that the public disclosure of this finding would have weakened the core of their philosophy, it is no surprise that the scholars chose to keep it secret. But one of them, so the tradition goes, Hippasus of Metapontum, broke the oath and disclosed the great secret, causing such a shock within the Pythagorean community that he was banished.

26 Monti and Wacks 2020.

27 Contemporary critics of the Pythagoreans' doctrine labelled it as supporting tyranny. See extensively on the topic: Burkert 1972: 118; Walter 1972: 118.

28 Seaford 2004.

Nonetheless, the need for secrecy was neither an absolute commandment nor an 'irrational' manner by which to protect a religious creed. In a critical re-reading of the motives that caused the schism among the Pythagoreans, Philip Horky points out that the contrast between *acousmatic* (the 'conservative' wing, linked to the aristocracy) and the *mathematical* (the 'progressivist' soul of the movement), about the will to promote the sharing of the until-then secret knowledge, was political rather than 'just' a matter of philosophy:

> The exoteric figures described by Timaeus are not said to promote their democratic causes or to publish the secrets of the Pythagoreans for the sake of self-aggrandizement or fame … Instead, there are two goals to these activities … the denunciation of oligarchical Pythagoreans before the people of Croton and the democratization of arcane Pythagorean knowledge.[29]

Like Hippasus, Gnaeus Flavius lived in the 4th century BC and, as secretary of the Consul Appius Claudius, he had access to a carefully guarded secret: the formulas to enforce the law and the calendar to perform such actions.

> The law had, in fact, become, after the publication of the twelve plates in the forum back in 450 BC, and after their disappearance in the fire of the Gauls, a secret prerogative of the priests, who kept the formulas and the calendar, i.e. the law and its time. The calendar was divided into favourable (*fas*) and inauspicious (*nefas*) days. In the latter, the proceedings for *legis actionem* could not take place, but only the priests, who held the office for life and had a monopoly on writing, knew what were the good and bad days and what formulas to apply. The exercise of the right was thus reserved for the knowledge of time. With the theft of the formulas and the calendar, Roman law, first exposed in public and then hidden, was directly made available through the text of the twelve plates.[30]

Whether Flavius disclosed only the *fasti dies* calendar or also the collections of *actiones* (the formulae that had to be cast as a spell to commence any legal process) known as *Jus Civile Flavianum* is still a matter of debate among the scholars of Roman law.[31] However, few doubt that the Roman jurist contributed to solving the issue presented by the rhoticism of Latin. Not being able to spell the correct *formula* precluded the *actio legis* from

29 Horky 2016: 124. For the Pythagoreans not worshiping aristocracy, see Rowett 2014: 112.
30 Catanzariti 2014: 1.
31 Santoro 2002: 293–366.

proceeding, and as a consequence, failing regardless of the merits of the case. Knowing when to litigate and how to render the appropriate formula affected the exercise of public power. The Roman bureaucratic apparatus was more oriented to preserving its power rather than considering the needs of the people. Nonetheless, after the *Jus Civile Flavianum* became public this apparatus lost part of its control over the *actiones*.

The *res gesta* of Hippasus and Flavius can hardly be compared to the social control techniques of the modern bureaucracy. However, their history obviously reminds us of Edward Snowden and Bradley Manning, the American 'whistle-blowers' who in 2013 stole and published classified information. In both the past and present cases, at least at first blush, citizens have been empowered by the newly (and unlawfully) obtained knowledge, but a closer analysis hints at a different conclusion. Their acts had a negligible impact on society, compared with the consequences of Gnaeus Flavius' disclosure. Snowden and Manning's leaked information generated a public outcry. It also generated media frenzy about Big Brother and nurtured paranoia on social networks. Yet it was a flash in the pan; there has been no effective enhancement of political or judicial control of intelligence agencies and their tactics. In contrast, Flavius' actions gave citizens of the entire Roman Republic the genuine capability to access the law and reclaim the recognition of and respect for their rights.

In other words, the real question is whether the historical tension between secrecy and transparency can be released by conceiving an undefined 'right to be informed' or a 'right to transparency.' Moreover—recalling what Hobbes regarded as the objective of knowledge—one should ask whether these rights should be granted only if supported by an actual interest of the claimant.

In brief then, to 'know' about the *interna corporis* of power is a right in itself or, by contrast, should the State disclose its activities to guarantee accountability? Must the knowledge of State and governmental affairs be of some practical use for those who seek it? Or—more explicitly—when it comes to State and government affairs do we have a right to mere curiosity? Now that the State surveillance capability is scaled up to an unprecedented level of pervasiveness, this is far from a mere theoretical dilemma.

In a democratic society secrecy acquires a dialectic (though not a dichotomic) dimension. Citizens are supposed to have 'rights'—i.e. from the politician's perspective, artificially built social pretences that can be denied with a snap of a finger because of the 'greater good'—to both 'know' the State's inner facts and not to have the State invade their personal sphere. Rulers, in contrast, have the raw power to hide themselves from the public's prying eyes and to orient public opinion by manufacturing its consent. Secrecy, therefore, becomes a *quid pro quo* in the relationship between citizen and political power, the rule of law and the separation of powers acting as go-between.

> If constitutional models are interpreted as primarily cultural models, secrecy becomes a lens through which social developments and normatively institutionalised procedures can be more deeply understood. Modern constitutionalism has, in fact, generally been placed at the foundation of the state community as an indispensable and binding pact.
>
> Well, the theoretical analysis of secrecy requires a precise reflection on the institutional links incorporated in modern constitutions: the use of secrecy in a democratic state depends in fact, on the constitutional composition of public and private prerogatives and the maintenance of the division of powers.[32]

In theory, the openness of the *res publica* is (formally) accompanied by the acknowledgement, to the advantage of the citizen, of the right to be protected from the prying eyes of the State, by the unscrupulous processing of their (apparently harmless) personal information, as well as by the private sector and by the stealing of their ideas through patent, copyright, and industrial secret protection. However, the right to privacy—the right to control one's personal information—is routinely questioned by public powers. Moreover, abuse and misuse of personal data is now a *fait accompli*, no matter what the 'law on the books' says.

As much as State secrecy is at the core of power, must be protected at all costs, and is annoyed by the 'petulant' assaults of watchdogs and civil society, citizens' right to secrecy and control over their own lives is not nearly so well protected. 'National security' has become the shortcut to silence abruptly any criticism against State-run surveillance programmes involving either real-time monitoring, data retention, or the processing of already available personal data

> An efficient and logically well-designed personal data management system, without (or with only limited) technical capabilities, has been shown to be extremely effective in achieving a comprehensive, large-scale 'management' of the citizens of a state, and others who represent a perceived threat to the state. Of course, the needs of public policing can be satisfied by the intrusion into the private life of an individual. Nevertheless, this very goal requires the processing of publicly available and, prima facie innocuous, personal information.[33]

32 Catanzariti 2014: 12.
33 Monti and Wacks 2019: 37.

It seems clear that in seeking to contain the contagion, miscalculations in the balancing exercise between the right to privacy and public safety and the public interest were made. Western governments generally adopted ineffective contact tracing strategies after having wasted precious time agonising about 'possible threats' to the 'right to privacy' and the risk of 'techno-control.'[34]

Power and transparency

The cultural role of secrecy in pursuit of an equilibrium between competing interests is more apparent when considering the differing approaches of Eastern and Western societies. England pioneered the idea of an 'open parliament,' as witnessed by the struggles that finally in 1803 led the press to be allowed to report the proceedings of parliament and the publication of Hansard. Its influence spread throughout Europe, and the transcription of what was said in the political arena soon became standard practice. Even revolutionary Russia recorded the Communist Party Plenum sessions which were eventually made publicly available.[35]

The publicity of parliamentary sessions, though, serves mainly political needs. In liberal democracies it gives the appearance of providing a check on what the legislators are doing. It also allows politicians to conceal their actual motives for supporting legislation or institutional reform. Actual decisions are taken elsewhere, be it the cabinet, the leaders of political parties and private stakeholders, or in the secrecy of diplomatic activities. Transparency, in short, is a tool to achieve its exact opposite. Under authoritarian regimes 'openness' is a way to deliver political messages or, more often, direct accusations to friends and foe.

If modern parliamentary sessions respect (at least formally) the notion of openness, this is not necessarily the case for the administrative machine of a State. Once a piece of legislation is passed, it does not belong to Parliament anymore as the apparatus of the public administration—the executive—takes over. Bureaucracy is a fundamental component to secure the survival of the State. Ministers come and go, but bureaucrats stay forever. Hence the importance of a well-organised system of properly trained civil servants. The French *École Nationale d'Administration* is an obvious recognition of the importance of the role of the civil service.

A well-tuned administrative mechanism, though, does not imply that its design, function, and outcomes should be made public. In a complex society the 'proceduralisation' of administrative law and the mandatory documentation of the grounds for decisions are principally ways to prevent local

34 Ibid: 132.
35 Kramer 1999.

bureaucrats from building autonomous and unaccountable power. But this does not necessarily imply the right of the citizen to be a watchdog of the State. Hence, there arises the political dilemma of whether—and if so, to what extent—to expose bureaucratic decisions to public view. Transparency is generally perceived as the banner of Western democracies, as much as secrecy is seen as a necessary evil. However, the interaction between the two is considerably more complex and nuanced.

Freedom of information (FOI) statutes passed in many jurisdictions empower civil society to expose political and criminal wrongdoing. At an abstract level, transparency provisions are found in many countries of both hemispheres. Nevertheless, there are important differences in regard to the *cultural* attitudes toward secrecy and transparency. As much as it may seem counterintuitive, 'transparency' and access to information (or prohibition against concealing it) were and are also practised by authoritarian regimes.

Under the fascists in Italy, Article 41 of the Royal Decree no. 965 of 30 April 1924 declared:

> [E]ach professor must diligently keep the class newspaper, on which he shall progressively record, without cryptographic signs, the profit grades, the subject explained, the exercises assigned and corrected, the absences and failures of the pupils.

Similarly, in the post-WWII, democratic Italian Republic, the discipline of ham radio operators prevented them from 'speaking in code.' It required the use of only four languages so that the surveillance offices of the then-Ministry of Posts and Telecommunications could check that ham radio operators did not use the medium for illicit purposes, mainly related to running terrorist rings. The reasons for these regulatory choices are clear: the State—or rather, the executive—must always be able to control what happens, from the microcosm of a classroom to the ethereal world of electromagnetic waves.

The Chinese freedom of information act is a clear example of how transparency can also be directed at controlling the inner workings of public administration. The legislation is extremely useful to authoritarian rulers as a way to keep at bay their chain of command. The concern that a freedom of information act might endanger national security is at the core of the decision adopted by China to open the door on local rather than national law-making institutions:

> The Chinese government faced a choice whether to first introduce FOI law or FOI Regulations … FOI law has advantages compared with FOI Regulations. It can create a new and enforceable access right and impose criminal sanctions against violations of disclosure requirements … In March 2004, the Internal and Judicial Affairs

> Committee of the NPC recognized the need to adopt FOI law in China in order to supervise government agencies and safeguard the public's rights to know, participate and supervise. It added that the State Council was drafting FOI Regulations, and that FOI law would be enacted based on the experiences learnt from the implementation of the Regulations. This indicates that FOI Regulations would be adopted before the adoption of FOI law.[36]

Interestingly, though, China rejected the idea that free speech is part of freedom of information, the latter being a way to control the activity of public administration rather than recognising an individual right of access to information. In other words, by adopting a law-based administrative process, the Chinese government appears to have sought closer control of the activities of civil servants rather than granting its citizens an instrument to facilitate democratic participation in the administrative life of the country:

> The Constitution of 1982 empowers the people to criticize and make suggestions to any government agency or official, to make complaints and charges against, or exposure of, any government agency or official for violation of the law or dereliction of duty. To exercise this constitutional right, the people need a right to know. However, Chinese reformers recognized that reliance on the link between FOI and freedom of expression under the Constitution only encouraged more resistance to FOI reform, especially after the failure of glasnost reform in the former Soviet Union.[37]

This claim is far from uncontentious. The apparently acceptable explanation is that FOI legislation is used by the central government to strengthen bureaucratic control. This assertion belies three decades of administrative law reform.[38]

It is hard to deny that the preservation of social stability is a major limitation of the application of the right to access information:

> The Regulation on Open Government Information [ROGI] created an unprecedented right of access to information with the potential for improving administrative accountability, but established a peculiar exemption of social stability. 'Stability maintenance' has long been an overwhelming political task for Chinese state organs, and has profoundly affected legal practices, posing a challenge to

36 Xiao 2018: 76.
37 Ibid: 43.
38 Xiao 2011: 51.

> judicial control of abuse of the aforementioned discretionary exemption. Added to the challenge is the obscurity in the standards for judicial review of discretion … The ROGI … grew out of a special Party-state context. In particular, the ruling Chinese Communist Party (CCP) has instructed the state apparatus … to adhere firmly to the principle of maintaining social stability … Long before and along with implementation of the ROGI, local governments have resorted to the mechanism of 'social stability maintenance' … a key component of which being information control, when facing growing social discontent or public protests.[39]

Unlimited access to information plainly jeopardises peace and security. Therefore access to information is allowed only when it does not endanger the maintenance of 'social stability.' Judicial review of the denial of access is based on principle rather than rules, thus allowing the ruling party absolute control over what may be disclosed.

A similar 'dual-use' approach is evident also in the 2009 Russian Federal Law entitled 'On providing access to information on the activities of government bodies and bodies of local self-government.' Article 29(4) of the Russian Constitution declares:

> Everyone shall have the right to seek, get, transfer, produce and disseminate information by any lawful means. The list of information constituting the state secret [sic] shall be established by the federal law.

Only with the enactment of the 2009 Federal Law has it been possible to put the right to freedom of information into effect. The real-life exercise of this right has, however, proved to be difficult because of the requisite cumbersome bureaucracy and the lack of citizens' confidence in the recognition and enforcement of this right:

> *FreedomofInfo* noted little coverage of the Act's passing in the mainstream media, despite the interest of FOI and human rights NGOs: 'There is still a great deal of scepticism … due to the historical lax attitude to law among Russian bureaucrats and the prevailing culture of corruption.'[40]

39 Chen 2016: 81.

40 Constitutional Unit International Focus: Russian Federation, University College London, https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/international-focus/russian-federation (visited 12 January 2021).

Moreover, in a perfect twist of the publicly declared goal of the legislation, the use of an access request—and in general, the watchdog role performed—by NGOs has been exploited to label some as 'foreign agents.'[41]

The Indian National Right to Information Act of 2005 is a paradigmatic example of how deeply rooted cultural and social attitudes can reduce the effectiveness of a statute. In this caste-based society, the enforcement of the act met with the resistance of the upper castes[42] and, it has been suggested,[43] of corrupt bureaucrats.

The Japanese transparency and secrecy regulations are no less interesting from the perspective of the interaction between cultural roots and (imported) laws. Whatever the norm may be, a culture of secrecy such as exists in that country has other ways to sanction the breach of confidentiality not only of State secrets.[44] Obviously Tokyo has pursued a different path from Beijing in the enactment of transparency laws. Nevertheless the result is strikingly similar. Modelled upon the US Freedom of Information Act, and passed in 1999, the Act on Access to Information held by Administrative Organs[45] is the Japanese equivalent.

Transparency is instrumental in securing the government's accountability rather than creating a 'right to know.'[46] This was admitted in 2012 by Article 25 of the Act for Establishment of the Nuclear Regulation Authority.[47]After less than a year, though, the Japanese Parliament passed the Act on the Protection of Specially Designated Secrets.[48] The government was afforded the power to classify information secrecy levels. It acquired the discretion to decide the classification without the need to define legally the concept of national security.

Japan did not enact the law to influence the judiciary to enforce the right of transparency, but, once the government puts the seal of secrecy upon information, a court is highly unlikely to question the decision:

> [The bureaucrats] will designate too much information as 'special secrets' so that their decisions won't be scrutinized or second guessed until they are dead. What we know from various scandals

41 'Freedom Info Russian FOI Organization Declared Foreign Agent,' 4 September 2014, http://www.freedominfo.org/2014/09/russian-foi-organization-declared-foreign-agent/ (visited 13 January 2021).
42 Sharma 2015.
43 Peisakhin 2011.
44 Sieg 2016.
45 Act n. 42 of 14 May 1999 http://www.japaneseselawtranslation.go.jp/law/detail/?id=99&vm=04&re=01 (visited 3 January 2021).
46 See Miyashita 2010.
47 Act n. 47 of the 27 June 2012, https://www.nsr.go.jp/data/000067231.pdf (visited 3 January 2021).
48 Act n. 108 of 13 December 2013.

> is that bureaucrats have often decided against the public interest and now have a way to hide their misdeeds.[49]

Moreover, the State secrecy law attracted harsh criticism for its potential to limit free speech, media freedom, and the accountability of government officials by punishing whoever leaks a State secret:

> The National Public Service Act (NPSA) might also have the effect of placing a restriction on reporting or speech. Article 100 punishes a national public officer for leaking government secrets, and Article 111 specifies punishments for persons who 'instigate' government officers to divulge secrets.[50]

The Japanese situation is interesting in both its political dimension and the foreign influence behind the enactment of the law. The country has a long-standing tradition of information exchange with the US. Recently the question has arisen of whether it should join the 'Five Eyes,' the intelligence network whose nodes are the US, the UK, Australia, New Zealand, and Canada.[51] However, an essential condition for the widening of the intelligence alliance is the adoption, by Japan, of 'adequate measures' to avoid the country becoming the weak link in the information chain, thus putting the entire network at risk. But Japan does not appear to be especially keen to become a full member of the network, opting instead for some sort of 'special status.'[52] The State secrecy law has been a way to address US apprehensions about Japan's capacity to protect Western-actioned intelligence. It is noteworthy, however, that the focus of American concerns and the subsequent Japanese legislation is on creating a system of more robust provisions to render leaks a criminal offence, a topic that is of utmost sensitivity for the Americans.

The US Freedom of Information Act[53] allows direct access to whatever declassified, non-public information[54] is held by the administration, with no

49 Pollman 2015.

50 Jitsuhara 2018: 172.

51 Herman, Arthur, 'Time for Japan to Join the Five Eyes.' *Nikkei Asia* online edition 12 September 2018, https://asia.nikkei.com/Opinion/Time-for-Japan-to-join-the-Five-Eyes (visited 3 January 2021).

52 Abe, Daishi Miki, Rieko, 'Japan Wants de facto "Six Eyes" intelligence Status: Defense Chief.' *Nikkei Asia* online edition 14 August 2020, https://asia.nikkei.com/Editor-s-Picks/Interview/Japan-wants-de-facto-Six-Eyes-intelligence-status-defense-chief (visited 3 January 2021).

53 The Freedom of Information Act, 5 U.S.C. § 552, https://www.justice.gov/oip/freedom-information-act-5-usc-552.

54 Not all kinds of information are accessible under the FOIA's regime, which includes nine exemptions and three exclusions. Exemptions include, inter alia, classified information

need to state a specific reason. However, its real-life application is not so straightforward. When it came to prosecuting authors of leaks to the media, the relationship between the US intelligence community and other branches of government, namely, the Department of Justice, revealed its complex nature. According to the Bayh Report of 1978:

> Many of the 'leak' cases have not been investigated by the FBI because of the Department of Justice's policy of refusing to investigate unless the intelligence community is willing to declassify all information related to the case. This policy grew out of frustration by the Department over the years with intelligence community reluctance to provide necessary evidence to prosecute major leak cases after the FBI had invested considerable time and effort in investigation.[55]

The Report also provides useful information about the attitude of the US intelligence community toward the risks of a judicial order to disclose classified materials as a part of a defence strategy aimed at exposing classified information:

> Prosecutors in the Department of Justice and intelligence community officials have always recognized that the espionage statute is not an effective remedy for all 'leaks' to the newspaper … because of the counterproductive disclosure of further secrets. The Department of Justice is also aware that a defense counsel, in the course of trial or through pretrial discovery, can threaten the Government with discovery motions or a line of questioning that requires the disclosure of classified information … So long as there is a real threat that prosecution of the defendant may reveal sensitive information in the course of a trial, he or she may engage in this 'gray mail' to avoid prosecution.[56]

A few years later, though, in a striking similarity with its Russian counterpart, the American administration seriously considered restricting the

---

for national defence or foreign policy, trade secrets and confidential business information, inter-agency or intra-agency memoranda or letters that are protected by legal privileges. Exclusions apply to law enforcement and national security records. US Department of State, Freedom of Information Act, https://foia.state.gov/Learn/FOIA.aspx (visited 20 February 2020).

55 US 95th Congress (1978) National Security Secrets and the Administration of Justice US Government Printing Office. p. 7. https://www.cia.gov/library/readingroom/docs/CIA-RDP94B00280R001200030003-0.pdf (visited 14 January 2021).

56 US 95th Congress (1978) *cit.:* 11.

extension of the Freedom of Information Act by excluding intelligence-related information and exploring the possibility of regarding those who seek declassified information as in itself amounting to criminal intention. This occurred in the case of James Bamford, author of *The Puzzle Palace*, the first and most authoritative book on the US National Security Agency. Bamford exploited the whole repertoire of investigative journalism. He did not limit his search to filing FOIA requests. He also targeted retired NSA members and entered the lion's den by 'hanging out' in the NSA lobby, doing nothing but eavesdropping on the conversations of intelligence operatives waiting to be granted access. Moreover, wandering around NSA public spaces, he succeeded in collecting NSA-related vehicle number plates.[57] His book was, at the time, explosive:

> Declassified documents in the Central Intelligence Agency's archives show that while the CIA was looking to include the Freedom of Information Act in its war on leaks, the National Security Agency was seriously considering using the Espionage Act to target *Puzzle Palace* author James Bamford for using FOIA. While Bamford has briefly discussed this on a handful of occasions, the declassified memos and briefings from NSA confirm that this was more than just an intimidation tactic or a passing thought – the NSA had truly wanted to jail a journalist for his use of public records. When the Agency determined that this was unlikely to happen, they moved on to exploring other legal avenues which could be used to punish Bamford for his FOIA work.[58]

He also successfully sued the NSA. His FOIA request led to the exposure of some 6,000 declassified documents. The NSA finally complied; however, as a last line of defence it shuffled the papers before making them available to the journalist.

During the pandemic, similar 'bureaucratic creativity' was evident in the response of both the UK and Italian civil services to the attempt by two NGOs seeking information about the involvement of major US technology companies in the design of the digital infrastructure to manage the pandemics in Britain, and about the record of the scientific committee that formulated the lockdown policies adopted by the Italian prime minister.

57 Bamford 2021.

58 North-Best, Emma, 'NSA Wanted to Use the Espionage Act to Prosecute a Journalist for Using FOIA.' 24 October 2017, https://www.muckrock.com/news/archives/2017/oct/24/nsa-bamford/ (visited 15 January 2021).

The UK's Freedom of Information Act,[59] like its North American counterpart, does not require a specific reason to request the civil service to release documents and information. But when the government signed a major agreement with a number of Big Tech companies and other less known business partners, it kept the contents of the contracts 'confidential.'

> On 28 March 2020 the British Government announced its strategy to use various technologies 'for coordinating the response with secure, reliable, and timely data—in a way that protects the privacy of our citizens—in order to make informed, effective decisions'. The ambition of the programme was considerable as was the quantity and quality of information to be processed … On 5 June 2020 the civil rights media organization openDemocracy announced that it had obtained a part of the agreement between the British Government and four high-tech companies (Microsoft, Google, Cambridge Analytica partner Palantir, and Faculty).[60]

Initially, the British government refused to disclose the details of the deal in response to the NGOs' access request. Only when *openDemocracy* threatened legal action did it disclose the documents.[61]

In Italy, during the peak of the pandemic the measures taken by the executive to contain the contagion were determined by a 'techno-scientific committee' whose records were kept secret for no apparent reason. In April 2020 *Fondazione Einaudi*, a transparency-supporting NGO, filed a request for the disclosure of the committee records relating to meetings held between 28 February and 9 April 2020. These were meetings where the total lockdown and other restrictive measures were recommended to the executive. The government acknowledged the committee's suggestions by mentioning them in the presidential decrees that shut down the country. Originally the government denied the access request, but *Fondazione Einaudi* successfully sued and the executive granted the requested access. This occurred prior to the Consiglio di Stato (the court of appeal for trials involving the public administration) issuing a final decision on the appeal filed by the government that lost at first instance.[62]

59 Freedom of Information Act 2000, http://www.legislation.gov.uk/ukpga/2000/36/contents (visited 20 February 2020).

60 Monti and Wacks 2020: 101–102.

61 Fitzgerald Mary, Crider Cori, 'Under Pressure, UK Government Releases NHS COVID Data Deals with Big Tech.' 5 June 2020, https://www.opendemocracy.net/en/ournhs/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/ (visited 18 January 2021).

62 F.Q. Desecretati i verbali del comitato scientifico. Fondazione Einaudi: 'Palazzo Chigi ha inviato la documentazione, accolto nostro appello.' 5 August 2020, https://www.ilfattoquotidiano.it/2020/08/05/desecretati-i-verbali-del-comitato-scientifico-fondazione-einaudi-

But this developing story was not as straightforward as it may first appear. At trial the government justified its decision to maintain the confidentiality of the committee's records by raising procedural arguments, claiming that they were merely 'general administrative documents.' The Administrative Tribunal for the Lazio Region held that it provided no substantial reason to support its claim that secrecy or confidentiality would protect either public or private interests. On appeal, the government advanced the argument that secrecy was warranted to protect public order and security. It requested a delay of disclosure until the emergency expired.

The contradictions in this argument are obvious. If there is an actual risk to public order and security, the records should *never* be made public. If the records were susceptible to disclosure once the emergency has been lifted, this would clearly be on political grounds. Why, then, did the government change its mind so abruptly and release the documents? The answer lies in the intricacies of Italian administrative law and the cavalier use of presidential decrees beyond their formal role. Both courts pointed out that the prime minister lacks the power to issue temporarily binding orders. In other words, he does not have the authority enjoyed by the US president to issue executive orders. If the Council of State followed up its preliminary ruling, it would have almost certainly affirmed the illegitimacy of the governmental decrees. The disclosure of the committee records did not require the appeal to be pursued any further. The matter was dismissed and the Council of State did not issue its final decision on the legal validity of the presidential decrees. By releasing the records, in other words, the executive went into damage control mode. It sought to use presidential decrees as policy-enforcement instruments irrespective of the alleged (non-existent) danger to public order and security.

To return to the Bamford debacle, the attitude of elements of the US intelligence community was, as mentioned, similar to that of their Russian counterpart; the main difference was that Bamford did not suffer any retaliation or threats to his life. His best protection was not a single provision or an article of the US Constitution. His safety was safeguarded by an entire system based upon rule of law, where checks-and-balances facilitated the handling of highly sensitive material without being silenced by the use of blunt instruments. It demonstrates the fact that no single provision enabled the effective use of the right to transparency. It was the legal *zeitgeist* of the country as a whole that acted as a catalyst to produce the desired outcome. The relationship between a shared rule of law, democratic culture, and the technicalities of a legal system obviates the need for formalistic rule-based approaches.

palazzo-chigi-ha-inviato-la-documentazione-consultabili-da-domani/5891394/ (visited 18 January 2021).

There remains, however, an unacknowledged elephant in the room: the leak of classified information to the media and, in general, to the public. Access to non-secret or declassified information is a powerful tool available to civil watchdogs and, as shown, the government cannot depend on being 'protected' by the courts. Leaks, by contrast, are a horse of a different (shady) colour. They may occur because a member of the 'inner circle' has a (spontaneous?) crisis of conscience. This may be part of a deliberate strategy to expose enemies. They also represent, of course, a powerful weapon in political struggles. The legal status of national security leaks is always controversial. Exposing the violation by governments of human rights abuses may not warrant punishment. But to compromise or undermine State secrets and thereby imperil national security cannot be condoned. The impact of leaks on national security is the subject of the following chapter.

4

TECHNOLOGY AS DISRUPTOR

While science might be neutral, technology is not. The discovery of atomic energy was an extraordinary attainment, susceptible to infinite applications. But when unleashed as a nuclear bomb, the nature of the achievement was transformed forever.

Technology is inherently purposive. The safety mechanisms of a single-action Colt 1911 are designed to prevent accidental discharge. Once the weapon is cocked and loaded and the safety catch is effortlessly removed by a swift hand movement, it can do only one thing: fire. A Beretta 92 (M9, in US military language), on the other hand, is designed to force the shooter to think before pulling the trigger. Safety is disengaged with a counterintuitive movement: the thumb must push the safety lever upward, while the hand, by contrast, closes. The double-action makes pulling the trigger more difficult. It gives the soldier a fraction of time to think before firing. A Glock 17 embeds the safety in the trigger itself. Accidental discharges are therefore unlikely to happen, although if loaded, the gun can fire without the need for thinking about any complex movements. The science behind these armaments—ballistics—is the same. Its conversion into a tool or instrument changes according to the will of the engineer.

The idea that the technology of information could—and should—be built either to enforce surveillance and control, or to evade them was well understood by national security government experts and computer-savvy activists. It has evolved from the niche of spies and hacker domains into legislation dealing with both issues. Building law enforcement-friendly telecommunications devices is a requirement in many countries. By contrast, GDPR of 2016 made data protection by default and by design a mandatory requirement of every personal data processing platform.

While politicians debate the balance between freedom and national security, members of two mythical groups, the National Security Advocates and the Privacy Guardian Party, took the matter into their own hands. The former developed software technologies to impose clandestine surveillance and intrusion into individuals' personal domain. The latter countered with

 DOI: 10.4324/9780367809775-4

computer programmes and platforms granting anonymity and offensive capability.

Crucial to this matter is the debate about data-gathering technologies and encryption. This (once) obscure branch of mathematics is now at the heart of intense dispute and controversy. It allows people to be uniquely tracked and, through digital rights management systems, controlled in what they can and cannot read, listen to, and watch. Through propaganda and profiling it can alter their belief and behaviours. But it can also render their private lives 'tamper proof' to any public or commercial snooping attempts. It licenses the anonymous condemnation of misconduct. It empowers people to fight back.

Cryptography, disorder, and security

Cryptography is the archetype of the weaponisation of knowledge itself. It was once a technology without a theoretical background. Caesar's cypher was an ingenious method by which to secure his communications. But he devised the ruse out of a practical need, not as the outcome of scientifically validated research. With the passage of time, cryptography has changed its nature. It was elevated into a science whose applications were mainly available for military, diplomatic, and high-level business. In the US it attained the status of a military weapon. As such it was included in the category of 'dual-use technology' and subjected to strict regulation. However, the role of cryptography in the civilian world was soon transformed from an innocent diversion or intellectual challenge to a *political* asset.

The freedom instinct carved into the DNA of US culture together with the spread of (relatively) affordable and powerful computers and the *free* availability of mathematical research on cypher algorithms allowed an (initially) small group of people to use cryptography as a *defensive* tool against the prying eyes of the government. An exemplar is the case of Pretty Good Privacy (PGP), the (then) powerful encryption software that in 1991 sparked heated controversies and judicial proceedings in the US for its being made available outside the US by its creator, thereby endangering 'national security.'[1] Free access to PGP was considered by politicians, intelligence, and law enforcement agencies a gift to criminals and terrorists. However, there have since been a number of similar 'embarrassing' discoveries of backdoors or other hidden decryption methods embedded into commercial and even diplomatic communication products. They were sneaked in either by secret agreements with manufacturers or by publicly lobbying for their mandatory embedding.

The 'total war' of intelligence agencies against the public availability of encryption technologies was not only waged with covert and subtle

1 Monti and Wacks 2020: 90.

operations. It also included the development of weakened algorithms and the attempt to embed them into ordinary products by manufacturers.

The *Crypto AG* scandal, described by *The Washington Post* as 'the intelligence coup of the century,'[2] is a paradigmatic covert example. Since the end of World War II and until 2018, the Swiss-based company made its name as the manufacturer of highly secure communications devices based on state-of-the-art encryption technologies. Its clients were government and other international bodies. *Crypto AG*, though, was not a private business. It was jointly run by US and German intelligence services. Until the truth was revealed, the two countries spied on both friend and foe.

Tampering with communications products and software did not end there. Sometimes it was carried out by openly proposing the adoption of weakened products. In other cases, the weakness was 'purchased' as a hidden feature to be embedded into algorithms and computer programmes. An example of the first strategy was the Clipper Chip case. Between 1993 and 1996 (the year of its demise) the NSA advocated the use of the 'Clipper Chip.' It promised, according to the US agency, to secure digital communication using a sophisticated encryption algorithm. To make it possible it was necessary to install this cryptographic module in both the transmitting and the receiving devices. In other words, to make the chip effective would have required computer and telecommunication manufacturers to embed it by default in their products. However, the Clipper Chip included a key-escrow feature allowing law enforcement and intelligence agencies to unscramble the communications. The Clipper Chip, notwithstanding the bipartisan support of US politicians—including the Clinton Administration[3]—never found a home in the motherboards of computers and other electronic communication devices. Its use was challenged by civil rights advocates such as the Electronic Frontier Foundation and the Electronic Privacy Information Center, and computer experts such as Matt Blaze, Yair Frankel, and Moti Yung, who managed to detect serious vulnerabilities affecting its promised 'security.'

An example of the other approach (seeking to covertly poison the strength of encryption-based security software) is the NSA–RSA secret agreement exposed by Reuters in 2013 after the Snowden leaks.[4] According to news

2 Greg Miller, 'The Intelligence Coup of the Century.' *The Washington Post* online edition 11 February 2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ (visited 29 January 2021).

3 The White House Office of the Press Secretary Statement of the Press Secretary 4 February 1994, https://epic.org/crypto/clipper/white_house_statement_2_94.html (visited 29 January 2021).

4 Joseph Menn, 'Exclusive: Secret contract tied NSA and Security Industry Pioneer.' *Reuters News Pro* 20 December 2013, https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220 (visited 29 January 2021).

reports, RSA—a world-renowned cryptography firm founded by the creator of the public key encryption algorithm—entered into an agreement with the US National Security Agency to insert into a widely sold product called 'BSafe' a tiny, almost invisible, feature that would have allowed to the *cognoscenti* an easier cryptanalysis.

The (alleged) necessity to weaken or even forbid the use of encryption outside 'good guys circles' never lost its momentum. About 20 years after the Clipper Chip debate, in 2015, the then British Prime Minister, David Cameron, sought to ban strong encryption from users' communication devices. He requested the support of the then-President Obama for US companies to work with British intelligence. Although his wishes did not appear to be granted, in 2016 the UK Parliament passed the controversial Investigatory Powers Act, later declared by the High Court to be in violation of EU laws. This was complemented in 2018 by the Data Retention and Acquisition Regulations.

More recently, the EU has begun to question its 'absolute' commitment to protecting fundamental rights:

> Two leaks, one published by Politico[5] and the other by StateWatch[6] suggest that Europe is considering restricting the use of cryptography in the private sector and/or seeking ways to circumvent it. In particular, as the analysis conducted by the American Electronic Frontier Foundation remarks, the idea would be to block end-to-end encryption, i.e. encryption that is performed locally, on the user's terminal, or circumvent it before (and regardless of whether) the message goes through a public communications network. The reasons behind this choice are – years later – still the same: 'fight terrorism' and 'protect minors'; and years later they continue to be even more difficult to sustain than in the past, both in legal and political terms. Moreover, following up these proposals would, paradoxically, have disruptive effects on the management of national security.[7]

5 https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf (visited 29 January 2021).

6 Council of the European Union Draft Council Declaration on Encryption Security through Encryption and Security Despite Encryption, 21 October 2021, https://www.statewatch.org/media/1434/eu-council-draft-declaration-against-encryption-12143-20.pdf (visited 29 January 2021).

7 Andrea Monti, 'Crittografia, tutte le contraddizioni dell'Europa.' Formiche.net online edition 20 Novembre 2020, https://formiche.net/2020/11/crittografia-europa-sicurezza/, available in English at https://blog.andreamonti.eu/?p=1893 (visited 29 January 2021).

The target of European legislators is end-to-end encryption, a technology that scrambles a message on a local computer *before* it is sent. Therefore, if a person eavesdrops on the communication, confidentiality is still protected when the encryption is sufficiently robust. The solution discreetly and (still) unofficially whispered by the EU is dubbed 'client-side scanning' (CSS). In short, CSS is a system that 'intercepts' content locally (i.e. on the user's computer) before the end-to-end encryption starts working. Through a mechanism of 'marking' and blacklist matching, CSS decides if the content in question is legal or legitimate (a not insignificant difference) and, if not, blocks it by reporting the fact to the authorities. It is clear that, in this case, the use of cryptography would be irrelevant because the check would take place before the content is hidden.

CSS has old roots. The decades-old, boiling-frog-like commercial strategy by large software houses has almost been accomplished. Nowadays, it is perceived as normal that, in order to work, a communication device must be 'registered' with the manufacturer's systems and that the manufacturer can, remotely, know what the user does with it. Anti-virus software is also based on the principle similar to that of client-side scanning, i.e. the search in the files present on a computer for 'signatures' matching those present in the threat database.

Summing up, it is clear that the prerequisite for the large-scale acceptance of CSS is already there. Nevertheless, this scenario does not necessarily suggest that the European solution will succeed because, regardless of its practical feasibility, there are political limits that would be very dangerous to cross. The CSS mechanism raises concerns about threats to human rights and the abuse of the technology by States. It is not difficult to think of a system that from the original objective ('protect minors' or 'fight terrorism') is quietly reprogrammed to block political or social dissent, even in the absence of a danger to public order and security.

While the debate continued between these two positions, similar to the irresistible force paradox, the availability of the Internet to a worldwide user base changed, for the third time, the role and nature of cryptography. Encryption has become what makes digital society work. Once the Internet became instrumental in the remote interaction of citizen, institutions, and companies, encryption technologies proved crucial. They made transactions over insecure channels safe and not refutable. They certified the integrity of messages and the identities of users and websites. They watermarked content shared online.

It is precisely this last exploitation of encryption technologies—content watermarking or, more accurately, digital rights management—that made the pendulum swing back to a repressive enforcement of cryptography. Digital rights management (DRM) is performed through a set of different technologies having encryption at their core. It allows the monitoring of the circulation of digital content (whatever its nature) across different

computers and prevents its unauthorised use. DRM is a highly questionable answer to legitimate copyright protection. This copyright-protection method drives the protection in favour of copyright holders, unfairly limiting fundamental rights. Legitimate users have the right not to be monitored when they read a book, watch a film, or listen to a piece of music. They have the right to use a copyrighted work, under the various fair-use doctrines, for teaching and research purposes. They are entitled to quote a protected work to exercise the right to free speech. Such rights are denied thanks to these technologies. It is not surprising that a vast anti-DRM movement has flourished to defeat DRMs and, in general, what was considered a repressive use of cryptography methods. Nor is it unexpected that US and EU legislators enacted statutes criminalising even the simple proof of concept of DRM-defeating methods. In other words, they banned freedom of research.

This is a crucial—and more general—point in the debate on technology as a disorder enabler. As will be explained later, the more a government (or private company) pushes to outlaw certain technologies, the more it fuels acts of rebellion as a growing social reality. Thanks to the wide availability of knowledge and tools to exploit it, individuals and groups can expose abuse and create instruments to oppose what is perceived to be an abuse of power. As counterintuitive as it may seem, the powers-that-be are no less responsible for technology being a disorder enabler. They continue to act on the assumption that, one day or other, their 'citizen-protecting programmes' will eventually be exposed. Until that moment, they operate undisturbed notwithstanding the suspicions of civil rights activists and independent technology experts, systematically confirmed by leaks and media investigations.

The technology of whistle-blowing

There are, as suggested in the previous chapter, numerous motivations for the leaking of information. It may be because a concerned citizen (a civil servant or employee) finds it impossible morally to continue under the unconscionable conditions he or she is enduring. Sometimes leaks are fed to the media by politicians seeking to undermine or hurt their party's 'friends' or foes. Occasionally it is in pursuit of personal gain. In other cases, leaks may be done to affect the economy, as in the case of 'rumours' about impending mergers and acquisitions, or, by contrast, the abrupt sale of a company, allowing profits to accrue to the *cognoscenti* and losses to the rest. Finally, they may be part of the propaganda and disinformation arsenal of a State.

In contemporary society leakers are generally 'tolerated' despite the institutional outrage that accompanies every betrayal of confidentiality. The 'right to leak' may also be officially sanctioned. Whistle-blowing has become socially accepted and, in various jurisdictions, it has even acquired legal recognition by which the exposure of alleged wrongdoing of a private entity or civil service is not prosecuted and, in some cases, the whistle-blower's

anonymity is protected. Anonymous denunciations are a widely acknowledged instrument of transparency and justice. However, there is something intrinsically disturbing about accusing an individual of misconduct while staying hidden without the opportunity for the victim to refute the allegation.

The tumultuous—and, finally, murderous—relationship between US Congressman Frank Underwood and *Washington Herald*'s reporter Zoe Barnes, the fictional characters of the American TV series, *House of Cards*, epitomises the role of leaks. It asks the fundamental question: does the truthfulness of the disclosed information and the public interest override the personal motives of the leaker?

But what is a 'leak'? The conduct of Gnaeus Flavius was, by modern standards, a leak. But a breach of confidence and the reporting of hitherto unknown facts to a public authority fall within this category. Keeping informants who expose syndicates, cartels, and organised crime safe is of crucial importance—hence, witness protection programmes. In an authoritarian society, however, political dissidents do not enjoy legal protection. However, even in democracies those who expose the wrongdoing of government and civil servants need protection.

More controversial, though, is the behaviour of those who disseminate information and launch accusations for their own personal advantage, the public benefit being either an afterthought or a side-effect. As with many other alleged so-called contemporary issues, these problems were debated more than a thousand years ago, within the arc of Roman rule, from the monarchy, through the Republic and the Principate. *Questiones perpetuae* were Roman criminal courts with jurisdictions over crimes of public concern such as bribery and electoral *combine* (*crimen ambitus*, *crimen sodaliciorum*), treason (*crimen maiestatis*), personal injury (*crimen de iniuriis*), and homicide (*crimen de sicariis et veneficis*: killers and poisoners). In the early life of Rome, a court could not commence a trial on its own. It was necessary for a reputable citizen to initiate proceedings by identifying the wrongdoer. These were the *delatores*. *Indices*, by contrast, were individuals who withdrew from a criminal enterprise and reported it to a magistrate with impunity as a *quid pro quo*.[8] In the late Republic and early Imperial era, *indices* and *delatores* were synonyms for 'a person who denounces a criminal act perpetrated by somebody else, without having received moral or material damage from it.'[9]

Making the *questiones perpetuae* aware of a crime was important. In the event of a successful indictment, *indices* and *delatores* were awarded prizes. Reporting crimes and sustaining the accusation were a public duty

8 Sciortino 2011: 50.
9 Petraccia 2014.

but also a way to obtain exposure to advance a political career (*gloriae causa*), vengeance, or as favour to another. It became an actual profession:

> When these two types of motivation coincided, the punitive model envisaged by the *quaestiones* worked in the best of ways; when, on the other hand, there was a clear prevalence of personal motives over the objective reasons for the judgement, this model then began to show the obvious symptoms of its imperfection.[10]

The abuse of this activity altered the public attitude towards *delatio nominis* for the worse. It was regarded with disdain. It led to the harsh punishment of *crimen calumniate*: slander. Although the matter is controversial, according to some scholars, during the Republican era slandering somebody with the accusation of having killed a relative (*parricidium*) did not warrant the usual sanction (the breaking of both legs). It had to be punished by a 'K' branded on the forehead. Offenders were required to bear the mark of *infamia*. They were barred from making any further accusations, and lost the possibility to profit from the prizes arising from successful indictments.[11]

Delatores (similar to their Athenians counterparts, the συκοφάντης[12]) were originally mainly reporters of 'serious crimes.' But later, Emperor Augustus made use of them as 'reverse-leakers,' i.e. informers. They were instrumental in exposing plots against his rule, breaking the boundary between crime reporting as a public duty and snitching as essential to preserve the ruling power:

> During Augustus's *Principatus*, therefore, delatores proved to be extraordinarily useful, especially to foil attempts to assassinate the Emperor and control the crowds. Perhaps it is also because of the spread of these methods that Tacitus states that, in the name of the security of the *Princeps* and the empire, freedom, already compromised by the first century BC events, ceased to exist altogether.[13]

Leakers v whistle-blowers

The history of FBI officer Mark William Felt, recently acknowledged to be the insider who led *The Washington Post*'s reporters Bob Woodward and Carl Bernstein to uncover the 1972 Watergate scandal, is instructive.

10 Centola 2016: 19.
11 Ibid: 23.
12 D'Amico 2018
13 Petraccia: 17.

It demonstrates how the professional media have played the role of civil watchdog by vetting information and protecting sources before releasing a story. It also offers insight into the role of personal creed as a motive that drives a civil servant to break the confidentiality seal of his job.

The story is well known. Apart from the investigation itself, the details have been the subject of books and a film. What has attracted less attention, though, is the motive of the informant and role of the US presidency. A contemporary *delator* (in the true Roman meaning of the word), Felt tipped *The Washington Post*'s reporters about the illegality of the unauthorised wiretapping of the Democrat National Committee headquarters in the Watergate Hotel. Long considered an ethically motivated whistle-blower, his reasons for exposing the FBI's activities have been questioned. Rather than acting for 'the greater good,' Felt leaked information to the press seeking revenge for not having been appointed head of the FBI after the death of John Edgar Hoover.[14] '*Gloriae causa*,' Cicero would have said. By contrast, he invoked the 'greater good' excuse (and the certainty that the higher part of the chain of command agreed with his course of action) against the accusation relating to Operation 'COINTELPRO' against American civil rights organisations. It is worth quoting it at length:

> The FBI's COINTELPRO—counterintelligence program—was designed to 'disrupt' groups and 'neutralize' individuals deemed to be threats to domestic security. The FBI resorted to counterintelligence tactics in part because its chief officials believed that the existing law could not control the activities of certain dissident groups, and that court decisions had tied the hands of the intelligence community. Whatever opinion one holds about the policies of the targeted groups, many of the tactics employed by the FBI were indisputably degrading to a free society. COINTELPRO tactics included:
>
> - Anonymously attacking the political beliefs of targets in order to induce their employers to fire them;
> - Anonymously mailing letters to the spouses of intelligence targets for the purpose of destroying their marriages;
> - Obtaining from IRS the tax returns of a target and then attempting to provoke an IRS investigation for the express purpose of deterring a protest leader from attending the Democratic National Convention;

14 Holland 2017.

- Falsely and anonymously labeling as Government informants members of groups known to be violent, thereby exposing the falsely labeled member to expulsion or physical attack;
- Pursuant to instructions to use 'misinformation' to disrupt demonstrations, employing such means as broadcasting fake orders on the same citizens band radio frequency used by demonstration marshals to attempt to control demonstrations and duplicating and falsely filling out forms soliciting housing for persons coming to a demonstration, thereby causing 'long and useless journeys to locate these addresses';
- Sending an anonymous letter to the leader of a Chicago street gang (described as 'violence-prone') stating that the Black Panthers were supposed to have 'a hit out for you'. The letter was suggested because it 'may intensify … animosity' and cause the street gang leader to 'take retaliatory action'.[15]

Felt authorised warrantless break-ins into private homes. He was indicted for these abuses,[16] but on 15 April 1981 he was pardoned by President Reagan. Why was the President willing to do so?

> I have granted full and unconditional pardons to W Mark Felt and Edward S Miller …
>
> To punish them further – after 3 years of criminal prosecution proceedings – would not serve the ends of justice. Their convictions in the U.S. District Court, on appeal at the time I signed the pardons, grew out of the good-faith belief that their actions were necessary to preserve their security interests of our country. The record demonstrates that they acted not with criminal intent, but in the belief that they had grants of authority reaching to the highest levels of government.
>
> America was at war in 1972, and Messrs. Felt and Miller followed procedures they believed essential to keep the Director of the FBI, the Attorney General, and the President of the United States advised of the activities of hostile foreign powers and their collaborators in this country. They have never denied their actions, but, in fact, came forward to acknowledge them publicly in order to relieve their subordinate agents from criminal action … America

15 Church Report *Cit.* Book II p. 10. https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf (visited 20 January 2021).

16 Horrock, Nicholas, 'Gray and 2 ex- F.B.I. Aides Indicted on Conspiracy in Search For Radicals.' *New York Times* 11 April 1979, https://www.nytimes.com/1978/04/11/archives/gray-and-2-exfbi-aides-indicted-on-conspiracy-in-search-for.html (visited 20 January 2021).

> was generous to those who refused to serve their country in the Vietnam war. We can be no less generous to two men who acted on high principle to bring an end to the terrorism that was threatening our nation.[17]

Reagan had read the court judgements and decided that the perpetrators did not have the *mens rea* to commit the offences, and that their actions were carried out in the actual belief that they served to protect the US, and that the rule of law must step back when major threats appear. His decision was, of course, within his power, but when national security was at stake, he drew a clear line that even courts are not permitted to cross.

At the other end of the leak spectrum are the modern 'civil rights whistleblowers' whose champions are Bradley Manning, Edward Snowden, Hervé Falciani, and, before them, their patriarch, Daniel Ellsberg. A brief summary of their conduct will provide the basis for the conclusions to be drawn in this chapter.

In 1971 Ellsberg disclosed a document which would become known as the Pentagon Papers, detailing US strategy in relation to the Vietnam War. A former analyst for the think-tank RAND Corporation, he became uncomfortable with the government's decision not to end the war. He sought assistance from a US anti-war senator who, after an initially positive response, turned him down. Ellsberg then approached the press. He faced more than a hundred years in prison, but was acquitted on the grounds of a mistrial after the court established that some of the evidence against Ellsberg had been obtained by an illegal break-in into his office. Ironically, or perhaps not, the trespassers were the same 'plumbers' who had bugged the Watergate Hotel.

In 2009 the name Hervé Falciani, an Italian-French computer expert, gained international exposure as the author of a massive leak of financial information he had extracted from the IT systems of his then-employer: the Geneva branch of HSBC. The so-called 'Falciani List' delivered a severe blow to the secrecy of the Swiss banking system and exposed a complex network of international tax fraud. Initially wanted by the Swiss police, he was arrested by the public prosecutor of Nice while, unbeknown to the latter, he was working with the *Division nationale d'investigations financières*.[18] Neither the Swiss nor the French authorities had any idea of the extent or merit of the allegations. However, when the facts were disclosed

17 Reagan, Ronald, 'Statement on Granting Pardons to W. Mark Felt and Edward S. Miller,' 15 April 2021, https://www.reaganlibrary.gov/archives/speech/statement-granting-pardons-w-mark-felt-and-edward-s-miller-0 (visited 20 January 2021).

18 Assemblée Nationale – XIV Legislature *Rapport d'information relatif au traitement par l'administration fiscale des informations contenues dans la liste reçue d'un ancien salarié d'une banque étrangère* 10 July 2013, https://www.assemblee-nationale.fr/14/rap-info/i1235.asp#P121_17804 (visited 25 January 2021).

to the French and (later) Spanish authorities they refused to send him back to Switzerland. Spain put him into a witness protection programme and, in parallel with French authorities, began investigating the names on the Falciani List. They shared information with other EU and foreign governments including Italy, the UK, and Greece. Magistrates discovered an entire system based on shell companies and sophisticated systems of tax evasion. HSBC was investigated and fined in various jurisdictions. The allegations ranged from supporting tax evasion to drug cartel money laundering and infringement of the Iran embargo.

Unlike Ellsberg, Manning, and Snowden, Falciani co-operated with the authorities. He became part of an intricate scheme to move his information from the dark side of an alleged crime into the glare of legally acquired evidence to be used in a trial.[19] The legal battle that erupted after the financial authorities started their investigation of members of the list provided important grounds by which to determine the legal status of illegally obtained information that is leaked.

Many defendants, charged after their names became public, unsuccessfully challenged the admissibility of the list because it was illegally created. Ignoring the doctrine of the 'fruit of a poisoned tree,' the French *Cour de Cassation* upheld the evidentiary value of the list in criminal trials.[20] Supported by a Byzantine argument, the Italian Supreme Court did not enforce the poisoned tree doctrine either. It ruled similarly to its French sibling. It held that, in principle, obtaining information under the international tax evasion treaty is not *per se* admissible evidence. However, since the list had been officially handed over by the French authorities to the Italian tax authorities, the latter had no duty to check either the reliability or the origin of the information. Therefore, the burden of proof that the information could not be admitted as evidence remained on the defendant.[21] The *Corte di cassazione*, though, mistakenly overlooked the fact that Falciani List came into the hands of the French authorities from two different paths. Initially it was passed to the DNIF by Falciani himself. Later, the list entered into the French judicial and administrative system through an independently (and legally executed) seizure by the public prosecutor of Nice. Therefore, precisely because the list was the outcome of a criminal offence, it may be admissible evidence.

This case raises three pertinent issues. Firstly, the author of the leak was, yet again, a computer expert who was granted access to the core of an entity's activities. Secondly, and yet again, he acted on ostensibly moral

19 Detailed information is provided in Falciani 2015.

20 Cour de Cassation criminelle, 27 November 2013, ric.13-85042.

21 Corte di Cassazione, sez. VI Civile – T, ordinanza 15–28 April 2015, n. 8605.

grounds, Finally, the leaker did not go to the media or the public. He collaborated from the beginning with the French authorities.

Chelsea Manning is the US military instigator of what has been called 'the biggest exposure of official secrets in American history'[22] for which she served seven years' imprisonment. In 2010 she contacted *The Washington Post* and the *New York Times*, but she was turned down. Only later did she approach *Wikileaks* and, finally, dropped a huge load of explosive information about US military actions in the Afghan and Iraqi wars. As in other cases, this one has been framed in the usual somewhat simplistic narrative of the insider who is unable to endure the facts she is witnessing (or is part of). It also sparked the usual flash in the pan of outrage and protests on the Internet, news, and broadcast media. But the reality is more complex. A moral dilemma undoubtedly determined Manning's course of action. But she also suffered from personality problems that contributed to the pressure that motivated her to leak the information. She did not take the precautions of a skilled information exfiltrator. She did not cover her tracks, or, if she did, she did it inadequately. Indeed, the investigation that followed her identification as the leaker found that she used her workplace computer to seek information about Julian Assange and *Wikileaks*.[23] The forensics on her computer revealed her conversations with the activists from the whistle-blowing platform. This evidence was discovered even though she made extensive use of freely available free-speech and privacy-enhancing technologies such as Tor and GnuPG.

In 2013 Edward Snowden, taking advantage of his privileged access to US National Security Agency secret activities, disclosed to the media the existence of classified information such as surveillance programmes. He did so by exploiting computer backdoors and mobile device weakness to eavesdrop on conversations around the world, including those of foreign political leaders. Unlike the cases of Ellsberg and Manning he fled the US to evade arrest, and found temporary asylum in Russia, despite the pressure and the protest of the US government that sought his return. He was therefore tried *in absentia*. Like Manning, he used GPG to encrypt his messages and TOR to secure communications with members of the media he tried to involve in the leaks. He also used *Off The Record*, 'a new protocol for protecting social interactions in the context of instant messaging'[24] granting secrecy and 'repudiability.'

While, at first blush, all the leaks recounted above appear similar, they differ in certain material respects. All originated in a breach of trust and a criminal offence, and all were justified morally as being 'for the greater

22 Nicks 2012.
23 Ibid: 131.
24 Borisov et al. 2004: 78.

good.' Yet, there is evident inconsistency in President Reagan's pardoning of Felt, and not of those who acted to advance or defend civil liberties. Is their whistle-blowing not pursued to uphold what they perceive as respect for the rule of law? Are they not acting to defend a greater good and expose corruption?

Morally, Felt, Ellsberg, Manning, and Snowden would seem to inhabit the same moral category; they exposed the abuse of power, even if Felt's motives were questionable. Nevertheless

> The cases should not, however, be read as giving a green light to citizens to steal and expose secret documents. Stealing government secrets cannot be any part of ordered liberty. Ellsberg was not vindicated; Ellsberg was the beneficiary of the inexcusable actions of an Administration increasingly untethered from the rule of law. An Administration that believed that the ends almost always justified the means.[25]

This is, however, not a simple matter. There is an obvious conflict between the need for State security and the moral duty to ensure that secrecy is not abused to conceal misconduct. Plato, in *Socrates' Apology*, may provide a resolution of the quandary. He argues that you may act according to your moral beliefs even if it is in violation of the law, but you must be willing to suffer the consequences. In other words, and at a more abstract level, when a leak of sensitive information occurs and the author is exposed, he may well be indicted for his actions. His moral motives should not affect the enforcement of the law. This would undermine the rule of law.

The Falciani List raises different issues. Falciani was unquestionably a whistle-blower but of private wrongdoings. His actions were unlawful as were those of his US accomplices. A Swiss court convicted him *in absentia*. The offenders are no different from members of a drug cartel or participants in organised crime who trade impunity for illegal and illegally gathered information. Falciani, however, was more similar to a *delator* rather than to an *index*. He was not part of the illicit conduct of his employee. He 'only' witnessed it. He sought justice, not compensation. Nonetheless, Falciani's legal status was decided according to political necessity rather than by enforcing a specific piece of legislation. Formally, he is still in the hands of the Spanish judiciary which refuses to extradite him to Switzerland. In cases such as his, sovereign States do not want to seal the leak; they want to *profit* from it.

Another important difference is that Falciani released a *targeted* leak against *specific* (alleged) wrongdoing similar to those of *Deep Throat*. Manning and Snowden, and to some extent, Ellberg, disclosed classified

25 Linder 2011.

information regarding governmental activities because they were *secret*, not because they were necessarily *illegal*. Moreover, they revealed an uncontrolled tide of information without prior vetting—hence the concept of 'deluge leaks.'[26]

The rational(ised) motives for deluge leaks typically occur where the leaker is disgruntled, in conflict with his employer, or seeking vengeance against the latter.

> The actions of deluge leakers are distinct from traditional whistleblower leakers. Certainly, some subset of the leaked records in recent deluge leaks were tied to government actions the leakers believed were illegal or improper, but the scope of the leaks went far beyond records that fit that description. The fact that leaked material includes voluminous records not implicated in any particular objectionable governmental action shows that the purpose of the leak is more than mere whistleblowing (even if that is one of the motivations), but also an action of protest against government secrecy or demonstration of the need for greater transparency.[27]

Technology and rebellion

There is, however, another perspective from which to assess the actions of these prominent contemporary leakers: the influence of the hacker/cyberpunk culture.

Between the 1980s and early 1990s, in the US and (mainly Northern) Europe there emerged an increasing ability to create digitally native information. The Internet provided the perfect vehicle for the exchange of information, and gave rise to the culture of hacking. Its *mantra* was 'information wants to be free':

> A rich bibliography flourished in this period, accounting for the birth of the hacking movement in the United States and Europe, the criminal and the digital underground, and the early development of the core concepts of the pro-privacy and anti-techno-surveillance culture as well as of the free-software and open source movements. It is not our purpose to provide a comprehensive history of the role of hacking in shaping the world as we know and experience it today. Suffice it to say, in contrast to received wisdom, hacking culture played a fundamental role in the development of the digital

26 Kwoka 2015: 1400
27 Ibid: 1443.

> industry and in the setting of the legal and political agenda in many countries.[28]

The call for *free* access to information was not meant—as a cursory reading of the word would imply—to be read as *gratis*. Theoreticians of the hacking culture venerate the idea the people should have unrestricted, unscrutinised, and uncensored access to knowledge. Richard Stallman, the MIT computer scientist who pioneered the idea of free software, explained the concept with an iconic line: 'free as in free speech, not as in free beer.'

Rebellion was (and remains) a core component of the hacking culture.[29] In parallel with Stallman's call for action to *free* the right to access and modify computer programmes' source code, this technological rebellion assumed other forms:

> A number of more militant computer aficionados around the country … believe that 'computer security' is a personal affront to their unalienable rights to access freely all electronically stored information (Landreth, 1985). To them pirating software, sharing passwords, illegally accessing remote computers, browsing through electronic files is not deviant behavior, but instead, the symbolic expression of their hostility to all large bureaucratic organizations that control informational or communication resources. To those who believe in the 'hacker ethic', the real 'criminals' in the world of computers are the private corporations, institutions, and governmental agencies who wish to deny access [to] or charge fees for the use of this wealth of information.[30]

This *über-mensch* attitude is perfectly captured in the film, *The Matrix*. It attained a cult status not only among the computer experts for its multi-layered meanings and for the characterisation of the heroes as human beings fighting a technological empire. Once connected to a reinterpretation of William Gibson's cyberspace, they acquired superhuman powers.

Distrust of the establishment was also the fuel of early crypto-anarchism dating back to 1992. Having privacy at its core, this ideology considered cryptography as the key to freedom from surveillance and tracking. The Crypto-Anarchist Manifesto, still available on a network resource of Massachusetts Institute of Technology, could not be more explicit:

28 Monti and Wacks 2020: 89.
29 Levy 1984.
30 Hollinger 1991: 9.

> A specter is haunting the modern world, the specter of crypto anarchy.
>
> Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner … These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.
>
> The technology for this revolution—and it surely will be both a social and economic revolution—has existed in theory for the past decade … But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable … The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy … Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property. Arise, you have nothing to lose but your barbed wire fences![31]

A few years later, in 1995, there surfaced the more complex, nuanced, and contradictory idea of *hacktivism*: the use of computer technology to foster political visions or civil disobedience. It eventually gave birth to international collectives such as *Anonymous*. But one question remains unanswered: how does society permit these individuals to engage in these activities? Is it really so easy to steal information even from the *sancta sanctorum* of national security databases? Is it worth investing billions worldwide into leak-prevention platforms, digital compartmentalisation, and physical and electronic workplace surveillance if someone like Chelsea

31 McCay 1992.

Manning is able to burn sensitive information onto a DVD and get away with it?

A possible answer comes from a well-known (and underrated) fact about the computer industry, brilliantly described by Alan Cooper in his *The Inmates Are Running the Asylum*.[32] Top management—and, by analogy—the top brass of the (national) security sectors do not pay enough attention to computer programmers. 'In the rush to accept the many benefits of the silicon chip, responsibility has been abandoned, and the inmates have been allowed to run the asylum.'[33] They are regarded as geeks living in their own world. Like the characters of the British sit-com, *The IT Crowd*, they are supposed to live in the basement and keep the computers running. They are invisible, and their superiors do not actually understand what they are doing. Worst, in the military, they do not belong to the 'operative culture', the one forged by arduous training that involves encountering lethal danger. Computer experts are allowed to do what they want because nobody cares to understand why things need to be done in the manner they prescribe. They live under the radar. That makes them dangerous. If this socio-cultural sketch is accurate it sheds light on an uncomfortable discovery: the protection of classified and sensitive information is, ultimately, in the hands of those who are on the mission to make them public. And free.

The connection between hacker culture and the war on (or obsession about) secrecy is well explained by Falciani himself:

> When people understand that power and secrecy are linked, they will want information to be shared … The attitude to be spread is that of the open source systems such as OpenOffice and Linux. The spread of these systems is a sign that the civil community made it possible to get away from historical manufacturers such as Microsoft. It is the proof that something can be done.[34]

For a very long time even democratic countries have kept their citizens away from core governmental issues. This task was (relatively) easy because the technology of information available did not allow its unaccountable and fast gathering, replication, and dissemination. It offered more control. The history of Vasili Mitrokhin, the Russian KGB officer who defected to the UK in 1992, is revealing. The Russian defector offered the UK government as a *bona fide* a stack of handwritten notes amassed during his 30-year career as a spy and asked, as a non-negotiable quid pro quo, for the documents to

32 Cooper 1999.
33 Ibid.
34 Falciani: 2195.

be publicly released. According to public records of the Mitrokhin Inquiry Report of the British Intelligence and Security Committee

> The Government decided that the best route to publish the material would be to approach an historian to research and collate the archive, with Mr Mitrokhin, and act as the editor for the published volumes. This approach, the SIS argued, would ensure that the SIS retained control of all the papers and that none would be published without FCO and Security Service clearance. The objective of the publication project was to place Mr Mitrokhin's material in the public domain in a controlled and unsensational manner.[35]

In short therefore, 30 years of handwritten Russian intelligence-related leaks were sealed under British government control in 1992. They were carefully revised and publicly released after their redaction in 1999.[36] Nobody questioned the authenticity of the leaks although they were Mitrokhin's statement of what was supposed to be in the copied documents. They were not stolen originals or their reproduction. And one may wonder, as in fact has been done, whether 'it does seem odd that a key KGB archivist never had access to a copying machine, but had to copy thousands of pages in longhand.'[37] To summarise, handling the deluge of information that 'came in from the cold' took time and, despite its extent, was easier to control. Some parts of the archive are still classified. None of them has so far been leaked.

Technology, activists, and the media

The modern whistle-blower ecosystem (Watergate, Snowden, *Cambridge Analytica*) demonstrates that the mainstream media have maintained their role as mediators between the shady world of deep throats and their righteous, avid readers' passionate interest in public and private conspiracies. But this is a remnant of the past because, thanks to the Internet, the process has become industrialised through the creation of leaking platforms. Whistle-blowers, dissatisfied civil servants, intelligence operatives, and State-sponsored propagandists need only upload their poisonous files to an online platform. Those who manage it will do

35 Intelligence and Security Committee, *The Mitrokhin Inquiry Report* Chairman: The Rt Hon Tom King CH MP Presented to Parliament by the Prime Minister by Command of Her Majesty June 2000, http://isc.independent.gov.uk/committee-reports/special-reports (visited 20 January 2021).

36 Andrews 1999.

37 Persico 1999.

the rest, informing the media that the next 'golden egg' has been laid. Information professionals need merely obtain it, scramble it, toss it into their media frying pan, and serve the public with their hot and spicy information omelette.

Of course, investigative journalism is by no means dead. The availability of leaks is useless if they are not interpreted and the leads are not pursued. Moreover, resorting to a middle-man to obtain a critical piece of information is not a straightforward process. The documents need to be vetted for their authenticity, their legal status must be assessed, and their political impact must be taken into account. However, that does not alter the key issue: public leaked-information brokers are now an essential part of the process. Compared with the scale, processing efficiency, and speed of circulation of the information made available through Wikileaks, the British treatment of the Mitrokhin archive appears trifling. The explosive combination of instant messaging, social networking platforms, and smartphones, not to mention the increased ability to communicate anonymously, has allowed critical pieces of information to blast into public spaces almost in real time. Critical pieces of sensitive information, as well as sordid political gossip, have been exposed to the glare of publicity speedily and without control. They are the new weapons of political warfare, either in close quarter combat, targeted killing, or tactical deployment.

In this new environment, Julian Assange and his creation, Wikileaks, cannot be underestimated. Wikileaks has changed the nature of the media from information creators to information consumers. It does not seek information. Like a pawnbroker, it weighs the value of what it is being offered, decides whether it is worth publishing, and names a price. It allows someone else to do the (dangerous) leg work. It does not deal with the source of information, only with the broker, whose duty is to protect the identity of his sources. By contrast, sources are confident that their identities are not going to be revealed by the broker, and are thus incentivised to leak the information. This description of the role of Wikileaks disturbingly resembles that of a 'fence,' a receiver of stolen property.

We may realistically conclude that leaks (of any kind and divulged for whatever purpose) are inevitable and unstoppable. However, public interest in the core activity of the State is no longer fuelled by a genuine watchdog approach. It is mostly motivated by prurient curiosity that generates flash-in-the pan reactions. Freedom of information laws are not enough to satisfy the appetite for secret or confidential information. Illegal leaks are the ultimate drug in the world of information. As in the world of narcotics, there is a constant need for replenishment and new products. Nevertheless, as in many cases of stimulating social involvement through computer technologies, after a voltage spike of public outrage the electric tension returns to normal. Like an electromagnet, once the media remove the plug from the socket, the force dissipates.

Technology, rebellion, and disorder

As mentioned, the free availability of computer technologies and, by contrast, the strict control over their enforcement are two sides of the same, disorder-enabling coin. Disorder is not—simplistically—caused by digital rioters or civil unrest promoters using smartphones and social networks. Disorder is also fuelled by the *machtpolitik* attitude of governments, the unscrupulous attitude of professional media, and by questionable business practices of the big-tech business.

To understand the role of technology as a 'disorder enabler' it is necessary to track the flow of information from the darkness into the light, to identify the points where its course is altered and how it occurs. A simple 'power graph' describes the relationship between the various forms of power enforcement and secrecy (or transparency). At one extreme lies 'maximum secrecy/national security,' and, at the other, 'maximum transparency/judicial power.' The enforcement of public order, in the middle, looks both ways.

What is 'judicial power'?

There are, of course, other variables. Public or hidden stakeholders—companies, pressure groups, and lobbyists—whisper in the ears of the powers-that-be. And organised groups of concerned citizens, collectives, and NGOs vocally reclaim their right to access secret information. The propaganda of foreign foes—rogue countries or terrorist organisations—is also part of the equation. More so than before, however, the relationship between these stakeholders has acquired a circular nature that makes the traditional stonewalling of information ineffective. Courts are supposed to be prevented from knowing details of intelligence operations. Citizens are deprived of information concerning law enforcement and national security activities. However, information is no longer compartmentalised, and the iconic 'FYEO' acronym has lost its James Bond connotations. Nevertheless, though, information leaks and short-circuits are almost routine. They are matters of 'when' not of 'if.'

Political decisions are challenged by acts of rebellion that would otherwise be near impossible to organise without the technology of information. The most obvious example is not only the creation of specific hacktivist instruments, but also the exploitation of computer programmes designed to perform innocuous tasks. In addition, the choices of the tech industry can (try to) alter the political equilibrium of a country without the need for governments to adopt formal measures.

An instance of the first category is the case of DNSet, a smartphone application developed in 2014 by Luigi Mancini and his team in Italy. In the second category are the intervention by Apple in the 2019–2020 Hong Kong

riots and the 2021 reaction of Signal to the Iranian blocking of access to the Internet.

A mobile operator controls all the network traffic generated by its customers. One of the main tools facilitating control is the routing all the Internet communication's requests through its own DNS. A DNS is a server that translates the domain name of a network resource into IP numbers, thus allowing users to reach their desired destination. A mobile operator can block its users' Internet access by denying the use of its own DNS. Mobile operators' DNS servers are pre-set in the smartphone and cannot be changed by users unless they own 'route access' to the device. As a consequence, governments seeking to prevent 'rebels' from organising, protesting, and publicising their actions merely have to order mobile operators to poison the smartphones' queries to their DNSs and kill them. Enter the Italian computer programme, DNSet, which permits the user to perform a simple, albeit crucial, operation: change the telecom operators' imposed DNS without having those administrative privileges that grant full control over the smartphone. In the paper describing the rationale behind DNSet, the authors of the software explain:

> In early 2014, the Internet censorship in Turkey has focused on social networks. Initially, a DNS Tampering attack has inhibited Twitter and YouTube websites; later, their corresponding IP addresses have been blocked at the IP level. This censorship of the Internet can be easily bypassed by skilled PC-users. Specific network configuration or software tools can circumvent this kind of censorship when you are browsing the Internet with a PC. Unfortunately, mobile users cannot mitigate such attacks with the same simplicity. Usually, Android users do not have administrator-level permits on their devices. In order to obtain such privileged permits, they have to hack their own device. This procedure is called rooting. Rooting allows users to overcome carriers and hardware manufacturer limitations, enabling advanced settings, the utilization of a larger-set of applications and other operations that otherwise would be inaccessible.[38]

Although DNSet was not intended as a political, censorship-circumvention tool, in 2014 the developers noticed an increasing number of installations from Turkey that reached a peak of 130,000 users. Upon further analysis of the data, they discovered that the applications coincided with the springtime protests against the Turkish Prime Minister, Recep Tayyip Erdoğan. It also emerged that a peak of uninstallations, about 2,000 requests, came from a

38 Mancini et al. 2014: 389.

device called '*Mehmet*' which was the name that the government had provided to students under a digital divide-reducing programme:

> We do not have any actual evidence to say that the automatic uninstallations were executed by the Turkish government without the users' approval, but our data confirm that some unusual uninstallation problem raised in Turkey approximately a month before the beginning of the censorship.[39]

A similar event transpired at the end of January 2021. As Signal, a secure, encryption-powered messaging computer programme started spreading in Iran, the government ordered the telecom operators to block the traffic. Signal's developers reacted by devising technical solutions to circumvent the ban. They asked users to set up proxies so as to divert the connections to a working Signal service. The difference with the DNSet case is that here the software support to a protest occurred ex post facto. In the Signal case, its developers took a political stand when it decided to disregard an order directed to third parties (the mobile operators) from a sovereign State, issued within its jurisdiction.

About two years before the Signal-Iranian case, between 2019 and 2020, protests erupted in Hong Kong. Concerns were raised about the demand from Mainland China that Hong Kong pass legislation to facilitate the extradition of persons accused of specific crimes to the mainland. Protesters resorted to HKmap Live, a geolocation app working on Apple smartphones to track police patrols. Apple denied the release of the app on its online store (the only way a computer programme can find its way onto an IOS device). The company claimed that it did not support illegal activities. By contrast, Microsoft, Twitter, and Zoom refused to hand over users' data at the request of the Hong Kong government.

Whatever the merits of the decisions, the problem is companies' *direct* involvement in international political questions. Of course, history shows that commercial interests have always played an important role in the intricacies of international politics, from the East India Company to the Cuyamel Fruit Company, not to mention the activities of the major oil companies in the Third World. But there is no longer a need for a strong connection with the interests of a State to enter the political arena of a country and take a stand against or in favour of the government.

Protests organised and managed through digital instruments owned by foreign companies are hardly contained through traditional policy techniques. In a democratic society it would be unthinkable to shut down the various content-sharing platforms, messaging systems, and telecommunication

39 Ibid: 393.

networks in order to control the lives of citizens. Should that occur, mesh networks created by low-tech devices and free software would still enable people to communicate freely. The only way for the State to exercise control over these activities would be to launch a massive, coordinated urban electronic guerrilla attack using local jammers to block the Wi-Fi transmission and disrupt the network by inoculating viruses and malwares. That would almost certainly provoke civil unrest that could only be contained with a heavy hand.

Disorder and the butterfly effect

Conventional protests' epiphenomena include activities such as loitering, riots, street violence, squatting, and, by the executive, the prevention of these social disturbances as well as the monitoring of political activities. In the last 15 years or so, however, intelligence and law enforcement authorities have been increasingly tasked to handle these matters not only on the street but also in the minutiae of computer programmes such as PGP and TOR and then online. Social networking and other forms of online mass gatherings, as well as the possibility to freely address a crowd and accord individual action symbolic status have reduced the boundary between legal protest and public disorder.

Borders no longer matter. They have dissolved in relation to commerce, personal relationships, and ending the lives of innocent persons. In a tragic example of the so-called butterfly effect an event occurring in Country A may rapidly spread around the world inflicting dire, unpredictable harm. On 3 February 2018 in Macerata, a small Italian town, Luca Traini, an Italian national, shot and wounded six African immigrants. He was sentenced to 12 years' imprisonment. He justified his act by claiming that he wanted to avenge the rape, homicide, and dismembering of a young, drug-addicted girl by a Nigerian drug dealer.

About a year later, on 15 March 2019, in Christchurch, New Zealand, an Australian national killed 50 Muslims, and wounded several others who were attending Friday prayers in their mosque. He broadcast the shooting in real time on his Facebook page. On one of the magazines of the assault rifle he had used, he wrote the name of Luca Traini.[40] He also claimed that he had been inspired by Anders Behring Breivik, the perpetrator of the 2011 Oslo and Utøya mass-murders who killed 69 people and wounded

40 Roberto Pavanello, 'Da Luca Traini a Sebastiano Venier, ecco cosa c'è scritto sul fucile del terrorista di Christchurch.' *La Stampa* online edition 15 March 2019, https://www.lastampa.it/esteri/2019/03/15/news/da-luca-traini-a-sebastiano-venier-ecco-cosa-c-e-scritto-sul-fucile-del-terrorista-di-christchurch-1.33687976 (visited 28 January 2021).

more than 300 in the belief that he was waging war against Islam in defence of Christianity.[41]

In the aftermath of the Norwegian murders, Breivik was discovered to have sent his lengthy political manifesto and a YouTube video to recipients based in the UK, Italy, France, and Germany just 90 minutes before the attack.[42] Instant and concealed social connections as well as immediate public visibility are the perfect match for those who foster civil unrest and terrorism. Internet exposure is an essential part of their plan.

Software and disorder

As much as the impact of social-sharing platforms and tools is nowadays a given in the literature on computer crime and national security, there is another aspect of the Breivik massacre that warrants deeper analysis: the role of software in influencing individual behaviour. Breivik declared that he honed his shooting skills by playing *Modern Warfare 2*[43] one of the instalments of the ultra-realistic first-person shooter videogame *Call of Duty* published by the American videogame publisher, Activision. In a Pavlovian reaction, some Norwegian shops removed the game and similar computer games from their shelves, only to return them once the negative public reaction had subsided. Of course, there is no direct connection between playing a violent, ultra-realistic videogame and real-life behaviour. However, it is generally agreed by those who played even the early pixel-art games on a ZX Spectrum, an Atari, or an old 486processor-powered PC—not to mention contemporary gaming powerhouses—that games are addictive. If played for excessive periods, too often they cause various effects, including confusing the game with reality. They alter the perception of the consequences of the players' actions.

The use of violent videogames as a military training platform is a contentious subject. They have been used for many years[44] in the creation of the perfect soldier until the use of remotely operated weapons—such as reconnaissance, spying, and striking drones—and high-tech platforms such as the

41 Jacob Aasland Ravndal, 'The Dark Web Enabled the Christchurch Killer.' *Foreign Policy* online edition 16 March 2019, https://foreignpolicy.com/2019/03/16/the-dark-web-enabled-the-christchurch-killer-extreme-right-terrorism-white-nationalism-anders-breivik/ (visited 28 January 2021).

42 Matthew Taylor, 'Breivik Sent "Manifesto" to 250 UK Contacts Hours before Norway Killings.' *The Guardian* online edition 26 July 2011, https://www.theguardian.com/world/2011/jul/26/breivik-manifesto-email-uk-contacts (visited 28 January 2021).

43 Helen Pidd, 'Anders Breivik "Trained" for Shooting Attacks by Playing *Call of Duty*.' *The Guardian* online edition 19 April 2012, https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty (visited 28 January 2021).

44 Huntemann and Payne 2009.

F35 jet fighter annihilated the distinction between a software-created world and reality. Of course, games such as *Call of Duty* can hardly be considered an actual training platform. But that does not rule them out of the game (no pun intended). They can be useful in the teaching of tactics, scenario evaluations, and other soft skills necessary in combat.[45] Moreover, they are instrumental in desensitising persons to violence and its effects,[46] not only among the military.[47]

Such an effect might also be exploited to achieve therapeutic effects. For instance, under the guidance of a professional, social environment simulation games can help to heal cognitive impairments[48] and negative personality traits.[49] Furthermore, an emerging trend is the idea that the digital moulding of human behaviour should not be limited to general purpose pieces of computer code. The result should rather be achieved through specifically designed software to be administered as a drug. The first hint of this trend emerged on 15 June 2020, when the US Food and Drug Administration approved the use of a specific attention deficit hyperactivity disorder healing videogame as a *therapy* to be prescribed for paediatric patients.[50] The experience with software faults and their consequences raises concerns.

Generally, the software manufacturing process passes through three phases. First comes the analysis, where the goals are determined, features identified, and the flow of information is channelled into algorithms. Then, in the development phase, the blueprints are turned into actual pieces of computer code. Finally, in the implementation phase, the software is integrated into a production environment. Once again, this description of the software's lifecycle sounds inaccurate to a computer professional. However, it is sufficiently detailed to point out where mistakes (or deliberate choices) happen. The history of software engineering is replete with examples of what

45 Scott Kuhn, 'Soldiers Maintain Readiness Playing Video Games.' 29 April 2020, https://www.army.mil/article/235085/soldiers_maintain_readiness_playing_video_games (visited 28 January 2021).

46 Grossman 2009.

47 Bastian Brock, Jetten Jolanda, Radke Helena, *Cyber-Dehumanization: Violent Video Game Play Diminishes Our Humanity* (2012). Journal of Experimental Social Psychology 48 491, doi:10.1016/j.jesp.2011.10.009 (visited 28 January 2021).

48 Edmund Lo Presti, 'Therapeutic Use of Life Simulation Games for People with Cognitive Impairments.' https://www.herl.pitt.edu/symposia/virtual-reality/presentations/LoPresti.pdf (visited 28 January 2021).

49 M. Colder Carras, M., Van Rooij, A. J., Spruijt-Metz, D., Kvedar, J., Griffiths, M. D., Carabas, Y., and Labrique, A. *Commercial Video Games as Therapy: A New Research Agenda to Unlock the Potential of a Global Pastime* (2018). Frontiers in Psychiatry, 8, 300, https://doi.org/10.3389/fpsyt.2017.00300 (visited 28 January 2021).

50 US FDA News Release, 'FDA Permits Marketing of First Game-Based Digital Therapeutic to Improve Attention Function in Children with ADHD.' https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-first-game-based-digital-therapeutic-improve-attention-function-children-adhd (visited 28 January 2021).

negligence in the manufacturing process can cause, from the 1998 explosion of the Mars Climate Orbiter, to the notorious Y2K bug that caused billions of dollars of damage. But the dreadful software fault that caused two Boeing 737 Max planes to crash, killing some 350 passengers, is the most revealing of the issues related to injecting digital parts into analogue bodies. The Boeing 737 Max had a hardware problem; Boeing's solution was cheaper than a physical modification: a software fix.[51] It turned out to be an inadequate—and deadly—one.

Secondly, and connected to the first question, is when the digital therapeutics software is released under a proprietary licence and nobody but the manufacturer and—perhaps—the involved national health authority can access the entire technical documentation. There is, in other words, no independent scrutiny, at least of the content of code. One might wonder why such a right of access should be granted. As in every trial, also in digital therapeutics the object of the test is the 'drug' efficacy and its adverse effects. A black box. As in the case of conventional medicines, if something 'unforeseen' happens, that fact is registered and sent back to have it resolved. However, nobody but the manufacturer can access this information.

Thirdly, if the software is designed to work on a distributed platform ('in the cloud' as the digital marketing experts used to call it) it would be a rather complex operation to put all the pieces of code together. It is the intrinsic *uncontrollability* of a computer-based society made of computer-mediated interactions, from the high level of the international economy down to the shaping of individual behaviours, that has a disruptive effect on national security.

Technology, disorder, and social singularity

A common feature of the phenomena that we are witnessing in the field of national security is the fragmentation of social compactness, caused by the unrestricted use of social media platforms. Individuals create swarms upon the basis of instant needs and occasional events. They unite, as in the several examples of 'cancel culture,' to 'protest' against an advertising campaign, a movie from the past, or a contentious statement issued by a public figure. Then, as a result of a reflex action triggered by 'privacy concerns,' they escape *en masse* by an instant messaging platform to join another system they do not actually know enough about because of its unique selling proposition, 'privacy abiding.' Then they become part of another shoal, to attack

51 Gregory Travis, 'How the Boeing 737 Max Disaster Looks to a Software Developer.' *IEEE Spectrum* online edition 18 April 2021, https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer (visited 29 January 2021).

a bigger fish in the stock exchange, as in the GameStop case which warrants brief consideration.

Toward the end of January 2021, a group of self-organised investors via the Reddit social platform managed to prevent speculative action on the stock of GameStop, a video game chain, by executing one in the opposite direction. The Goliaths of Wall Street had bet on the collapse of the stock of a company that was already in bad shape. By contrast, the Davids of the social platform began to buy shares, causing the stock to soar. As a result, the professional investors ran the risk of losing enormous sums of money, not because there were any rational or objective reasons for this (e.g. GameStop's stocks' incorrect value assessment), but because a (large) group of people emerged from nowhere, and used the same tools of speculation against them. Aware of the power they gained, these 'Amateur Internet Traders'—as the media haughtily nicknamed them—turned their attention to BlackBerry, another company that is not sailing in especially calm waters and whose shares then benefited from this sudden interest. Furthermore, in the usual Internet-like manner, the GameStop rally sparked imitation. Asian investors used the same tricks on the Malaysian stock exchange.

The financial world is wondering what the future scenarios might be because the GameStop affair is certainly not going to end and, probably, nothing will be the same unless legislators put a stop to these activities. Amateur Internet Traders simply employed the very same methods practised by professional stock market players. Why should they be prevented from doing so? Peculiarly, or maybe predictably, the traders have not been curbed by Wall Street internal regulations, a court warrant, or a presidential executive order. There was no legal ground to prevent a citizen from doing what investors have always been allowed to do. Rather these upstart traders were stopped by the companies that own the *software* they use to place their bets. Facing the GameStop storm, and claiming to have acted in compliance with market regulations, these brokers blocked these traders from buying and selling shares. Yet again (remote) control over a computer programme allowed a private entity to intervene in a matter of public interest.

Amateur Internet Traders might become permanent players in the stock market. 'Professional investors' would no longer be in control of the main asset of this sector: information. If a myriad of micro-investors organise themselves without going through traditional channels, no stock is safe, no investment strategy can withstand the uncertainty. In a word, it will cause financial chaos.

The media hastily hailed this affair as a victory for Internet users. It demonstrates, they said, the power of social networking platforms even against powerful institutions such as banks and hedge funds. But this is only partly true. The GameStop case is the latest example of an unstoppable trend made possible by the ubiquitous diffusion of the technology of information.

Cryptocurrencies

They are another example of the disorder-enabling role of digital technologies.

How cryptocurrencies work is a complex—although not difficult—topic.[52] It involves a solid understanding of Hayek's theory, of the basics of public key cryptography, and a technology-fuelled anarchism. In the aftermath of the Bretton Woods Monetary and Financial Conference of 1944, there was general consensus regarding the future of currencies. Banknotes lost their gold-backed status. They were traded as a *quid pro quo* not because of their *value* but because countries *agreed* to acknowledge that State-issued currencies were worth something.

Although, as Hayek advocates, there are no *per se* reasons to forbid private currencies, States continued owning the right to issue fiat money. For many years, monetary sovereignty has been an attribute of rulers. In some countries such as the US, local currencies are allowed on condition that the issuer pays his taxes in US dollars. However, this phenomenon is geographically and politically limited and lacks the capacity to leave the shores of its home country. Moreover, it replicated the mechanism of fiat money legal tender: a central issuer controls the creation of value. It can cause inflation or other monetary events without guarantees for those who accepted the private currency.

By contrast, cryptocurrencies such as Bitcoin succeeded in attaining worldwide success because of their different, rebellion-fuelled ideology. Cryptocurrencies are decentralised. Their quantity is mathematically predetermined. Nobody has centralised control over the creation of value or transactions:

> A cultural prejudice affects the debate on cryptocurrencies according to which the technological aspect takes precedence over legal analysis, which must systematically profess to be unable to understand the 'new' phenomena. In reality, this is not correct, and it is difficult – if we exclude the achievements of genetics – for the evolution of information technology to pose conceptually unknown problems to the jurist, and cryptocurrencies do not escape this observation. Letters of exchange date back to the 12th century and the Hawala, the Arabic equivalent, to the 8th century. Both served a function very similar to that of cryptocurrencies: transferring value without necessarily moving money. Moreover, when securities, derivatives, and other financial engineering objects took

52 Michael Nielsen, 'How the Bitcoin Protocol actually Works.' 6 December 2013, https://michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ (visited 30 January 2021).

> on an autonomous value, free from any link with reserves or currencies, it was evident that the 'King was naked,' and legal money was dead. On the contrary, it was artificially kept alive in a system that, thanks to the dematerialisation of information and value, no longer needs physical trappings to define and move wealth. The only real problem with cryptocurrencies is not legal but political and relates to the loss of State control over value and wealth. That is, ultimately, an instrument of social control.[53]

In broader terms, then, it can be said that centralised entities are losing their powers of self-organised and uncontrolled conduct. It is no longer a question of disintermediation between individuals and institutions. We are facing a progressive loss of their role.

Traditional (private) powers fought back. Private investors such as Tesla's founder Elon Musk took over the Bitcoin game by putting a huge quantity of 'traditional' money on the table. They purchased a substantial quantity of Bitcoin; hence they took control of its value, like in the 'traditional' fiat-money speculative game. They turned cryptocurrencies into an investment asset and made the latter lose their primary appeal: being separated and unaffected from the traditional monetary system. Moreover, the resources needed to keep the cryptocurrency infrastructure up and running (energy, mining factories, and so on) broke the decentralisation myth.

Exercises in direct democracy through online platforms, the organisation of protests against institutions and companies, the creation of economic value through cryptocurrencies, and now the taming of financial markets undermine the traditional systems of control and operation of a State, and the entire financial system. In short, the social contract is about to break down. There is no longer any need for the State, in exchange for sovereignty, to guarantee rights and economic value that can be secured by instruments outside public control.

But this newfound freedom from States and institutions is not real. The technologies that allow people to be 'unchained' from public powers are actually owned by other entities—Big Tech—that own the 'kill-switch.' They can make everything disappear at the snap of a finger. Also 'the community,' the unfathomable ghost summoned by political activists and technology enthusiasts as the key component of the 'digital liberation movement,' is not what it first appears. Behind any algorithm, computer programme, online platform, and digital project there is always only a limited number of people who own the knowledge to make things work. If they cease keeping the engine going, everything shuts down. They become the new rulers.

53 Andrea Monti 2018, 'A Contribution to the Analysis of the Legal Status of Cryptocurrencies.' *Ragion pratica, Rivista semestrale* 2/2018, p. 378, doi: 10.1415/91544.

We are facing, in other words, a situation where two different forces (Big Tech and the technological-driven anarchy) are undermining the existence of the political and economic system. Although this reconstruction sounds more like the plot of a political thriller, it highlights the need for the State to decide how to deal with this loss of power, which affects the very fabric of a nation. We should ask ourselves whether we are facing the drift of fundamental rights from a guarantee of social coexistence into individual claims against the State, whatever the cost. If so, we should ask ourselves how to stem it, even if the answer may not be pleasant.

The availability of a technological platform as well as of computer programmes efficient and secure to share leaks of whatever nature, to alter the economic stability and the exercise of political rights, is plainly a game changer. It poses the problem that lies at the core of this book. It challenges the idea that the technology of information should be available to the masses. It exposes the role of people—and private companies—in the management of national security choices, a question considered in the following chapter.

5

THE SUICIDE STATE

Previous chapters attempted to elucidate the role of technology in increasing the tension between State and citizen, and hence between power and rights. The massive convergence of economic, political, and technical developments has facilitated States exercising surveillance and behaviour control systems upgraded in power and speed although not necessarily in effectiveness. Governments will stop at nothing to collect information and raw data about almost anything and anybody. They seek to predict and influence human behaviour. This includes transferring criminal investigations and matters relating to national security, and the details and outcomes of trials, to automated systems or even to 'artificial intelligence' (AI).

By contrast, the same convergence turned previously unconcerned and isolated citizens into swarms of active players in the law and order/national security field. Online unrest apart, the anarchic delusion of being free from the State (as well as a misconceived 'right to privacy') led to the creation of a dystopia where choices are supposed to be taken by digital direct democracy, justice administered by on-the-fly social media juries acting as 'courts-and-hangmen,' where information springs from nowhere, and value is created by resorting to obscure mathematical algorithms. The State has lost its tactical superiority over the citizen because technology has become an equaliser, and cannot be effectively controlled or prohibited. Citizens can directly access tools that allow them to operate without the knowledge of the State and to render themselves resilient to State surveillance. The protection of individual rights through computer software is the main battleground where the interests of the State and citizens' rights clash. Anonymous Internet browsing protocols such as TOR, plausible deniability-ready encryption software, data shredding applications, fully anonymous email services, unbreakable messaging, and communication tools raise the question of whether these (mostly) freely available instruments are legally acceptable from a public policy perspective.

This black-and-white depiction of the current dialectics between citizen and power is, however, too simplistic and provides a not entirely correct reading of the matter. It does not take into account, indeed, the role of the Big-Tech

DOI: 10.4324/9780367809775-5

industry's business strategies and political goals. In the pursuit of personal gain, Big Tech moulded society according to its needs. They became the actual rulers, equipped to take on the most powerful countries of the world.

Countries with a market economy have a complex, intertwined relationship with economic and financial powers. The role of bankers and entrepreneurs is a constant in the operation of power relations. It is no exaggeration to say that multinational companies are powers in themselves. The dispute in 2021 between the EU and Big Pharma in regard to the delayed supply of the coronavirus vaccine speaks volumes. However, as much as companies operating in the financial, health, and other critical sectors play an important role in determining the political course of a country, nothing equals the power of Big Tech. Computers, computer programmes, and 'digital platforms' are ubiquitous. Network connections invade every aspect of society, from Internet-monitored refrigerators to cars, from remotely operated surgery to 'enhanced' weapons and troops. A substantial part of the world has been quietly lured into believing that there is no alternative to 'living connected.' Telecom operators actually 'own' the networks that are the battleground of 'digital anarchists' and public authorities. Financial institutions, capitalising on the technology of information, have already taken over the cryptocurrency bubble. Software houses have equipped computers and 'smart' devices with a remotely operated 'kill-switch.'

Who possesses the real power in a world inhabited by software and machines? The dilemma, in other words, is whether the issue requires a conservative, might-based approach—and therefore the *tout court* reaffirmation of the State's primacy—or a pragmatic recognition that the State has lost its exclusive 'grip' on national security and public order. A corollary and more theoretical question is whether the 'business' choices of those who control the technology of information determine the contents and limits of national security and public order.

The US is unquestionably the geo-economic and geopolitical centre of social-impacting technologies. US Big Tech created the computer industry for the public sector, then brought it to the masses—'the computer for the rest of us' was Apple's advertising claim of the 1980s. They turned the Internet into a mass market product and finally caged their customer-base in a technological walled garden with the creation of content-sharing and social networking platforms and, most important, with operating systems and software-powered smartphones and 'wearable technologies' that serve a different master from the individual who purchased it. All that would not have been possible without the help of the most powerful legal weapon ever created: copyright.

Copyright and national security

Copyright is usually associated with the illegal duplication and sharing of audio-visual works or unauthorised decoding of the streaming of major

sporting or entertainment events. Over time, in the name of copyright and claiming the need to protect authors, repressive pieces of legislation have been passed in various jurisdictions. The US Digital Millennium Copyright Act (DMCA) of 1998 implemented the 1996 World Intellectual Property Organisation's treaty that outlawed the circumvention of technological measures protecting copyrighted works. However, and notwithstanding criticism and, later, minor amendments, the core of the DMCA is to sacrifice other rights such as freedom of speech, education, and research to protect the interest of companies exploiting an artist's work rather than the authors themselves. It even punishes the simple releasing of a theory or a proof-of-concept that technical circumvention of these 'author-protecting' measures makes possible. It severely affects research on the security of cryptographic algorithms and their implementation.

The EU adopted a similar provision with its Directive 29/01 that allowed member States to pass specific provisions making it a criminal offence to market and sell such products, including pure research-oriented papers and computer programmes. The possibility—or, more accurately, the power—to exert total control over the *access* to software inner secrets was the flagship message of the US *Free Software Foundation* and other NGOs active in the technology of information sector almost everywhere in the Western world. They have foreseen better than anybody else the actual danger of such a reading of copyright laws.

Making the software inaccessible to public scrutiny allows the circulation of insecure and unreliable products. Zero-day vulnerabilities, design, writing, and implementation errors expose billions of connected devices to malfunctioning and deliberate attacks. Having the right to control how users interact with a computer programme and limiting their use are the pillars upon which the surveillance/behaviour-control society is built. It also empowers private companies—through 'cloud-powered' security services or the 'managed security services provider' business programmes—to take ownership of the critical infrastructures of an entire country.

In 1976 Microsoft's co-founder Bill Gates wrote an open letter to the US computer hobbyist community (*in pectore* hackers, actually) to complain about the 'illegal' circulation of the Altair BASIC, a computer programming language from which Gates and his business associates were trying to make a profit by selling it on a 'per-machine' base. It lay the foundation of a debate on future copyright regulations.

> As the majority of hobbyists must be aware, most of you steal your software. Hardware must be paid for, but software is something to share. Who cares if the people who worked on it get paid?
>
> Is this fair? One thing you don't do by stealing software is get back at MITS for some problem you may have had. MITS doesn't make money selling software. The royalty paid to us, the manual,

> the tape and the overhead make it a break-even operation. One thing you do do is prevent good software from being written. Who can afford to do professional work for nothing? What hobbyist can put 3-man years into programming, finding all bugs, documenting his product and distribute for free? The fact is, no one besides us has invested a lot of money in hobby software … Most directly, the thing you do is theft. [1]

A few years later, in 1983, Richard Stallman settled the basis for a diametrically opposed approach, lately evolved into the Free Software Foundation movement:

> I consider that the golden rule requires that if I like a program I must share it with other people who like it. I cannot in good conscience sign a nondisclosure agreement or a software license agreement.
>
> So that I can continue to use computers without violating my principles, I have decided to put together a sufficient body of free software so that I will be able to get along without any software that is not free.[2]

Different cultural approaches to software copyright directly affect the security of people and (critical) infrastructures that rely upon computer programmes. A partisan, business-only oriented reading of copyright, the DMCA, and DMCA-like statutes allow the enforcement of the 'security-through-obscurity' (STO) strategies. They are widely practised in national security circles, as explained in Chapter 4. By contrast, according to those who endorse an openness-based approach to copyright, STO does not actually fit well with the actual needs of national security, as pointed out by Bruce Schneier,

> Considerable confusion exists between the different concepts of secrecy and security, which often causes bad security and surprising political arguments. Secrecy usually contributes only to a false sense of security.
>
> In June 2004, the U.S. Department of Homeland Security urged regulators to keep network outage information secret. The Federal Communications Commission requires telephone companies to

1 Bill Gates, 'An Open Letter to Hobbyists.' *DigiBarn Newsletters: Homebrew Computer Club Newsletter* 3 February 1976, https://www.digibarn.com/collections/newsletters/homebrew/V2_01/gatesletter.html (visited 30 January 2021).

2 Richard Stallman, 'New Unix Implementation.' *net.unix-wizards, net.usoft* 27 September 1983, https://www.gnu.org/gnu/initial-announcement.html (visited 30 January 2021).

> report large disruptions of telephone service, and wants to extend that to high-speed data lines and wireless networks. DHS fears that such information would give cyberterrorists a 'virtual road map' to target critical infrastructures.
>
> Is publishing computer and network vulnerability information useful, or does it just help the hackers? This is a common question, as malware takes advantage of software vulnerabilities after they become known.
>
> The argument that secrecy is good for security is naive, and always worth rebutting. Secrecy is beneficial to security only in limited circumstances, and certainly not with respect to vulnerability or reliability information. Secrets are fragile; once they're lost, they're lost forever. Security that relies on secrecy is also fragile; once secrecy is lost there's no way to recover security. Trying to base security on secrecy is simply bad design.[3]

In short, this is the claim: STO does not guarantee long-term functionality and—as the continuous stream of security-related leaks shows—it can be beneficial in the (very) short term and in limited environments. However, STO does not guarantee *stable* control over the global security of an algorithm, software, or infrastructure.

Ideally, managing national security through obscurity should not even be considered. In a perfect world, software's source code would be designed and written with security in mind and carefully vetted in its implementation. Vulnerabilities of critical infrastructures would be mapped and fixed. Big Tech would be (legally) responsible for the products they supply to the public and the private sector (which are so interconnected that their difference is hard to see). In other words, as Schneier points out, 'Governments operating without accountability serve their own security interests, not the people's.'[4]

Security-through-obscurity is in fact a shortcut for carelessness and denial of responsibility. Software's source code can be inaccessible also to governments by making it available through its 'compiled' form (providing the cake, not its recipe). However, one may counter, the picture is not black and white. Access to the core of a computer programme is possible by way of 'fiduciary agreements.' They allow access to the software on a need-to-know basis and under carefully drafted non-disclosure agreements. Moreover, Big Tech is supposed to flank and support IT management to manage any problems that arise—for a fee.

3 Bruce Schneier, *The Non-Security of Secrecy*. Communications of the ACM 47(10):120, 2004, DOI: 10.1145/1022594.1022629 (visited 30 January 2021).

4 Ibid.

Reality, though, is a different world. There are routine and contingency security plans in almost any home affairs or defence ministry. Efficiency checks are supposed to be performed according to a predefined schedule. However, in many cases budget constraints (or mismanagement) route public expenditure toward more politically urgent, short-term goals. Actual 'prevention' is not always part of an efficient security model. The COVID-19 pandemic has exposed the huge difference between those countries where a culture of national security is taken seriously and those where 'security' is but a title on a forgotten report. Finally, the digital infrastructure of the Western world is more than 30 years old.

In the field of computer programmes, a preventive model based upon continuous checks—whether 'open source' or behind the curtain of a military precinct—does not actually work. Software is extremely complex, and it is simply unthinkable to examine it from scratch, especially without access to its 'blueprints.' Moreover, there is not just *one* piece of computer programme to review. There are many, starting from computer motherboards, the 'slates' where chips are soldered and circuits designed. They host several microprocessors. Microprocessors host firmware. Firmware is software. Software, also if it is hardcoded, can be exploited for malicious purposes. In 2018 *Bloomberg Business Week* published a report[5]—whose content was reaffirmed in 2021[6]—claiming that Chinese intelligence succeeded in tampering with the software code of US motherboard-manufacturer Supermicro Inc's Basic Input Output System (BIOS). According to Bloomberg, computer servers carrying the poisoned code were sold to major companies and important civil services' IT infrastructures. The Chinese government and Supermicro Inc. responded to Bloomberg pointing out the speculative nature of the articles. The matter remains unresolved.

A similar exemplary story is the *Spectre* and *Meltdown* vulnerabilities affecting a line of processors made by Intel, IBM, and ARM. It was revealed in 2018 that for decades computers equipped with these pieces of hardware were open to an esoteric vulnerability. There are no publicly documented incidents related to these two issues. Moving upward, similar issues affect the firmware of other essential components such as hard disks[7] and graphics

5 Jordan Robertson and Michael Riley, 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.' *Bloomberg Business Week* 4 October 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (visited 31 January 2021).

6 Jordan Robertson and Michael Riley, 'The Long Hack: How China Exploited a U.S. Tech Supplier.' *Bloomberg Business Week* 12 February 2021, https://www.bloomberg.com/features/2021-supermicro/ (visited 15 February 2021).

7 Kim Zetter, 'How the NSA's Firmware Hacking Works and Why It's So Unsettling.' *Wired Security* 22 February 2015, https://www.wired.com/2015/02/nsa-firmware-hacking/ (visited 15 February 2021).

cards.[8] Moving on toward the operating system, the more abstract layer of what makes a computer work, their source lines of code (SLOC) are measured in millions. The kernel of the Linux operating system is made by about 28 million SLOC, Microsoft's Windows 10 accounts for about 50 million SLOC, 2005 Apple OSX Tiger weighted over 85 million SLOC, and, in 2015, Google 2 billion.[9] Despite the use of automated vulnerability-spotters, flaws spurt from everywhere. The frequency and intensity of 'security updates' do not require further analysis. The matter is self-explanatory.

But a computer is not the only component of a network. There is a great number of 'smart' devices and computer programmes that are required to operate a network: routers, switches, firewalls, intrusion prevention and threat assessment systems, anti-virus and anti-spam, digital PBXes, authentication platforms, base transceiver stations. Blueprints and every single piece of equipment manufactured should be individually security-vetted. It may be possible, but is it feasible? Finally, if a government is given access to this unmanageable quantity of information, where should it find the expertise and the manpower to check *all* the hardware and software to be used within the national security perimeter in a reasonable timeframe?

The empirical evidence about this conundrum comes from the Italian legislation passed between 2019 and 2020 allowing the government to handle the threats to national security posed by Chinese Big Tech: Huawei's 5G technologies. Under the international public and diplomatic pressure generated by the US against the Chinese company,[10] Italy passed decree law 105/2019 (an act of the government issued under duress, turned into a proper law by Parliament in the form of the Law 133/2019). Among various provisions, the decree imposed a mandatory, pre-emptive security vetting of all devices and software to be deployed within the 'national security cybernetic perimeter.' It included critical infrastructures such power grids, aviation and transport, and health. The duty (and the power) to perform the vetting is given to the *Centro di Valutazione e Certificazione Nazionale* (the National Assessment and Certification Centre) that despite the urgency claimed by the government is still not operative at the beginning of 2021. By

8 Intel Corporation, 'Intel® Graphics Drivers Advisory.' 8 November 2020, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00369.html (visited 15 February 2021).

9 Metz, Cade, 'Google Is 2 Billion Lines of Code—And It's All in One Place.' *Wired.com* 16 September 2015, https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place/ (visited 15 February 2021).

10 BBC News—Tech, 'Huawei: UK Government Weighs up Ban of Chinese Firm's Telecoms Kit.' 6 July 2020, https://www.bbc.com/news/technology-53306809 (visited 15 February 2021).

contrast, on 7 August 2020 the government issued a presidential decree[11] to regulate how TIM, the former State-monopolist, should purchase Huawei's 5G infrastructure. It delegated to the private company the duty to perform the security checks and—astonishingly—allowed these security checks to be performed 'on paper' and according to the manufacturer's declarations. In other words, as a general principle the security of hardware and software to be used within the 'cybernetic perimeter' must be verified by a dedicated office of the civil service. However, the controls can be paper-based and, finally, delegated to a private entity. This is clearly a rather ineffective approach aggravated by the impossibility of excluding the 'cybernetic perimeter' from the rest of the networks. 'Cybernetic security perimeter-located' entities have to interact with the rest of the world. They cannot live in isolation. As in Poe's *The Masque of the Red Death* they think that they are free from any contagion. They are exposed nonetheless to plagues affecting the 'digital peasants' that live outside the castle and cannot be banned from entering.

Private business models, national security, and the kill-switch

The decree-law 105/2019 does not only (clumsily) regulate the use of digital technologies in critical sectors of the country. It also empowers the Ministry's Council President with a 'kill-switch' to shut down the Italian network. This is neither a unique power nor a novelty. Since 2009 the US administration and Congress started the political[12] and legal discussion to put the Internet Kill-Switch in the President's hands. Section 5.2 of an Executive Order issued to handle national security and emergency crisis made crystal clear that the administration had such power.[13] Cutting through legal hair-splitting, Egypt shut down the Internet and mobile network in 2011 to curb political protests,[14] as did Turkey in 2016, and many other countries have followed suit.[15] It is less known, though, that a kill-switch is also in the

11 Presidente del Consiglio dei Ministri. 2020. Decreto 7 agosto, https://www.infosec.news/wp-content/uploads/2020/08/DPCMHuawei.pdf (visited 15 February 2021).

12 Declan Mc Cullogh, 'Internet "Kill Switch" Bill Will Return.' *c|net.com* 24 January 2011, https://www.cnet.com/news/internet-kill-switch-bill-will-return/ (visited 15 February 2021).

13 The White House—Office of the Press Secretary, 'Executive Order – Assignment of National Security and Emergency Preparedness Communications Functions.' 6 July 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness- (visited 15 February 2021).

14 Matt Ritchel, 'Egypt Cuts Off Most Internet and Cell Service.' *The New York Times* 28 January 2011, https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html (visited 15 February 2021).

15 Jim Edwards, 'All the Countries Where Someone Managed to Shut Down the Entire Internet — and why they did it.' *Business Insider-Tech* 30 June 2019, https://www.businessinsider.com/countries-internet-shutdown-statistics-2019-6?IR=T (visited 15 February 2021).

hands of software houses and hardware manufacturers, and that its use is untrammelled but for business considerations.

In 2008 the *Wall Street Journal* reported a statement by then Apple CEO Steve Jobs acknowledging the existence, within their smartphone, of a hidden feature allowing the company to block any device:

> Mr. Jobs confirmed such a capability exists, but argued that Apple needs it in case it inadvertently allows a malicious program—one that stole users' personal data, for example—to be distributed to iPhones through the App Store. 'Hopefully we never have to pull that lever, but we would be irresponsible not to have a lever like that to pull,' he says.[16]

This feature later became a standard feature of every Apple device.[17] By empowering users to handle the switch Apple defused the controversy. Other manufacturers of hardware and software followed this path. The privately operated kill-switch is a *fait-accompli*. A lesser-known fact is that the widely spread subscription-based business model to use software and content can act as an effective kill-switch and it has been used as such.

National security and business models

In 2009 Microsoft Inc. launched the *Genuine Advantage Programme*. To work properly, Windows-equipped computers had to be remotely authorised by a software check of the 'legality' of the operating system and other Microsoft software installed (if any). Failing to pass the check prevented users from using the software, no matter whether they were using an unauthorised copy or if they had a legally obtained licence, not recognised by 'the system.' This DRM system (once again, copyright is the main force that regulates users' remote control) was dismissed with the release of Windows 7. It has been superseded by a user account-based mechanism, similar to those embedded into smartphones and tablets. Similar to Apple's OSX, for Windows 10 to work correctly, a user must own a 'Microsoft Account.' This account is the key to access other subscription-based software and platforms such as messaging, video-conferencing, and smart-working tools. As a consequence, the availability of software and platforms can be denied with the snap of a finger—or the press of a button.

16 Nick Wingfield, 'IPhone Software Sales Take Off: Apple's Jobs.' *The Wall Street Journal* 11 August 2008, https://www.wsj.com/articles/SB121842341491928977 (visited 15 February 2021).

17 James Cook, 'Apple Is Finally Turning on The iPhone "Kill Switch".' *Business Insider* 18 September 2014, https://www.businessinsider.com/apple-is-turning-on-the-iphone-kill-switch-2014-9?IR=T (visited 15 February 2021).

One of the companies that has made wide use of the subscription-based business model is Adobe. In 2013 the makers of Photoshop switched from a one-time licence fee to a subscription-based model.[18] Every time an Adobe software-loaded computer programme starts, a piece of software called the 'Creative Cloud' checks if the installed applications are up to date. Before this check, however, Creative Cloud ensures that the subscription is valid and that the computer is authorised to run the required software. If not, the applications do not launch.

The Executive Order 13884 dated 5 July 2019 by President Trump blocked the property of the Government of Venezuela.[19] As a consequence, Adobe started deactivating all the Venezuelan-located accounts, thus preventing regular users from accessing the software.[20] Later, access was restored thanks to a special exception issued in favour of Adobe.[21] But that does not alter the fact that the subscription-based, user account-activated business model was enforced to directly paralyze, in real time, a significant part of the activity of a country. Three aspects make the Adobe case relevant for the purpose of this book. Firstly, the 'kill-switch' imposed as a tool of foreign policy was deactivated because of business needs. Nonetheless, what happened is a clear warning to other countries: politically motivated sanctions can affect also the technological infrastructure and digital business and can target anyone. Secondly, if left switched on, the block would have also affected content stored outside Venezuela, 'in the cloud.' Thirdly, if recovered, content embedded in proprietary files could not have been opened because of the impossibility of using the necessary software, unless cracking it, thus breaking the law.

Another example is one of the battles fought in the soft war between the US and China. It involved the ban imposed by the Trump administration on Chinese companies such as manufacturers of 5G devices, computers, and smartphones, Huawei and ZTE (accused of threatening US national security), and drone maker DJI, accused of supporting the infringement of Chinese minorities' human rights. The first signs of the conflict were spotted in 2018 when AT&T declared it would no longer support Huawei

18 Christine Moorman, 'Adobe: How to Dominate the Subscription Economy.' *Forbes* 23 August 2018, https://www.forbes.com/sites/christinemoorman/2018/08/23/adobe-how-to-dominate-the-subscription-economy/ (visited 15 February 2021).

19 The White House—Office of the Press Secretary, 'Executive Order – Blocking Property of the Government of Venezuela.' 5 August 2019, https://www.federalregister.gov/documents/2019/08/07/2019-17052/blocking-property-of-the-government-of-venezuela (visited 15 February 2021).

20 BBC News—Tech, 'Adobe Shuts down Photoshop in Venezuela.' 8 October 2019, https://www.bbc.com/news/technology-49973337 (visited 15 February 2021).

21 Adobe, 'Cumplimiento de Adobe con la orden ejecutiva de EE. UU. | Venezuela.' 2019, https://helpx.adobe.com/la/x-productkb/policy-pricing/executive-order-venezuela.html (visited 15 February 2021).

devices. In the next two years the curve of the escalation grew fast and steep. Many other countries joined the US in banning (at least formally) Chinese manufacturers' access to core components of the national digital infrastructures, from 5G telecommunication networks to jointly operated data centres. None, however, pursued the goal with the determination of the US. Among the various actions taken, it is the technological ban enforced by Executive Order 13873 of 15 May 2019[22] that deserves to be analysed. The ban, confirmed to run until 15 May 2021, prevented Huawei from purchasing US technologies and hardware such as chips—microprocessors—powering the 'smart' devices. Additionally, it forced Google to revoke the licence rights over the Android ecosystem, embedded in all Chinese-made smart devices. As in the Adobe-Venezuelan case that ban has not been enforced in full. Existing users would have been allowed to continue to obtain apps and access services, and the kernel of the Android operating system, having being released under a *free* license (the GNU Public Licence), still allows its unrestricted use. By contrast, new users could not access *proprietary* software applications and services such as maps and email. Huawei countered the US move by developing its own smartphone operating system, Harmony OS, in case the ban was unlikely to be revoked. The final bullet has not yet been fired and it is too early to declare a winner. However, once again, copyright together with a business model based upon the constriction of the users played a major role in the game. Software is no longer used as a weapon. It has become a weapon in itself.

The Venezuelan and Chinese trade bans that included digital services (and the related business models) are exemplars of how the idea of a 'kill-switch' is not merely a software feature. It is a strategy that can be enforced in various ways and, therefore, may have many different faces. Another example is the business structure of managed security services provider (MSSP). In general terms, an MSSP is made of a security software manufacturer—such as, for example, an antivirus—that runs an online platform providing core services such as making available updates and upgrades or providing computational power to operate as a proxy that analyses digital files and internet access requests before allowing them to be used. The platform also deploys security software into the 'endpoints' (a marketing buzzword for users' computers) and controls the 'activation' (i.e. the payment of service fees). However, the management of the endpoints is not made directly by the manufacturer. It is delegated to a reseller who is given access to a control room connected to its own customers. In other words, the manufacturer and

22 The White House – Office of the Press Secretary, 'Executive Order Securing the Information and Communications Technology and Services Supply Chain.' 15 May 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain (visited 17 February 2021).

the reseller *access directly* all the computers behind a protective perimeter. As in the Adobe or Android cases, nothing would prevent the US government (or, actually, any government where Big Tech is involved) from issuing an immediate block of the managed security services provided abroad. By contrast, Big Tech might easily affect the security of a sovereign country (including its own) by deciding to dismantle a service, revoking *ad nutum* a licence on its own or, once again, under a direct order of a government, or denying the latter access to its own technology.

Neither Adobe nor Google capitulated to the government's demand. They successfully fought to obtain exemptions or limitations to the bans. Whatever the options, the implied assumption between a digital defence contractor or, more generally, Big Tech and its institutional counterparts is that they are into an *inter pares* negotiation. Several judicial decisions support this conclusion. For example, in 2016 the FBI took Apple to court because of its refusal to help the bureau access data contained in an iPhone. The court ordered Apple to provide a way to circumvent the encryption-based security of the smartphone's operating system.[23] Apple rejected the request on the ground that the security system was designed so that nobody, not even Apple itself, could circumvent it. Apple supported its position with an open letter to its customers stating that

> We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them. … While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.[24]

The matter was not resolved by a final ruling because the FBI found another way to crack Apple's security, thanks to the exploitation of an iOS defect. But that weakened the black-and-white Apple statement about the impossibility of supporting the FBI because of the robustness of the software. Apple's position looked more oriented to reassuring its customers—hence,

23 US District Court for the Central District of California. 2016. Case 15-0451M, https://www.justice.gov/usao-cdca/file/825001/download (visited 17 February 2021).

24 Tim Cook, 'A Message to Our Customers.' 16 February 2016, https://www.apple.com/customer-letter/ (visited 20 February 2021).

its profits—rather than to defending fundamental rights. After the San Bernardino case, another judge, this time in New York, ruled differently, denying Apple's duty to tamper with its products.

> In deciding this motion, I offer no opinion as to whether, in the circumstances of this case or others, the government's legitimate interest in ensuring that no door is too strong to resist lawful entry should prevail against the equally legitimate societal interests arrayed against it here. Those competing values extend beyond the individual's interest in vindicating reasonable expectations of privacy – which is not directly implicated where, as here, it must give way to the mandate of a lawful warrant. They include the commercial interest in conducting a lawful business as its owners deem most productive, free of potentially harmful government intrusion; and the far more fundamental and universal interest – important to individuals as a matter of safety, to businesses as a matter of competitive fairness, and to society as a whole as a matter of national security – in shielding sensitive electronically stored data from the myriad harms, great and small, that unauthorized access and misuse can cause.[25]

There are several interesting aspects of this decision. Firstly, the court corrected the order of the rights involved in the case. It affirmed that the core of the matter is not the right to privacy, but the extension of a warrant. This is consistent with a balanced approach to the right to privacy, not to be seen as a totem but as a dynamic legal notion interacting with other components of a legal system.

> When a court authorises a body-search or seizure of geolocation data, or the analysis of traffic data to establish a connection between individuals, it is misguided and superfluous to invoke a putative right to privacy. The bastions of a democratic society provide adequate protection in the shape of due process and the right to a fair trial. The appeal to 'privacy', for the reasons set out in Chapter one invites incoherence, uncertainty, and weakens the very right that it is sought to protect.[26]

Moreover, the court endorsed the notion that the government should not intrude into the manner in which a company runs its lawful business. It

25 US District Court for the Eastern District of New York. Case 15-MC-1902-JO 26 February 2016, https://www.govinfo.gov/content/pkg/USCOURTS-nyed-1_15-mc-01902/pdf/USCOURTS-nyed-1_15-mc-01902-2.pdf (visited 24 February 2021).

26 Monti and Wacks 2019: 49.

also gave prominence to the general interest to avoid unauthorised access to digital data. Once again, though, the problem was framed in the form of the 'Irresistible Force Paradox' and was not a decision on the merits. The judge decided on a procedural basis, ruling that it was not possible to use the legal remedy invoked by the State—the All Writs Act of 1789—to force Apple into supporting law enforcement. He evaded the core of the matter.

On 1 March 2016, a lower court in Sergipe, Brazil, ordered the arrest (later revoked) of Facebook's vice president for Latin America, accused of not cooperating in the retrieval of information exchanged via WhatsApp:

> Court officials said the judge in Brazil resorted to the arrest after issuing a fine of 1 million reais ($250,000) to compel Facebook to help investigators get access to WhatsApp messages relevant to the confidential drug-trafficking investigation.
>
> The move is likely impossible because WhatsApp began using end-to-end encryption technology in 2014 that prevents the company from monitoring messages that travel across its network.[27]

This case also reveals the same pattern shown in the Apple cases mentioned above: a company *designs* its services—or so it claims—so that they cannot be broken and, more important, does not regard a monetary fine as an effective incentive to comply.

In the same year, in Italy, news spread that Blackberry, whose focus was on communication security, had a different, more open approach to the matter. It helped Italian law enforcement to acquire suspects' chats[28] and cooperated with US authorities in drug-related investigations.[29] But it should be noted, firstly, that it *designed* its product to make users' messages accessible; secondly, it handed over to law enforcement the keys to decrypt the messages. The extent and the effects of the involvement of Big Tech in criminal investigations were apparent during the trial. Challenging the source of decrypted messages involving the defendants in a gang cartel trial, defence counsel succeeded in getting the prosecutor to admit that the messages were decrypted with the cooperation of Blackberry. However, it

27 Brad Haynes, 'Facebook Executive Released from jail in Brazil.' *Reuters – Media Industry* 2 March 2016, https://www.reuters.com/article/us-facebook-brazil-idUSKCN0W4188 (visited 15 February 2021).

28 Corte di cassazione Sezione III penale, 'Sentenza n. 10788.' 2016, http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20160316/snpen@s30@a2016@n10788@tS.clean.pdf (visited 25 February 2021).

29 Dave Seglins, Matthew Braga, and Jeremy McDonald, 'BlackBerry Hands over User Data to Help Police "Kick Ass," Insider Says.' *CBC-Technology and Science* 9 June 2016, https://www.cbc.ca/news/technology/blackberry-taps-user-messages-1.3620186 (visited 25 February 2021).

was not 'the usual support' that other private entities were used to provide. Blackberry gave the Royal Mounted Canadian Police the master-key, the *passe-partout* capable of opening any digital safe containing secured information. The defence tried to escalate the matter by seeking to have details of the master-key made public. The court denied the motion.

> Alan Treddenick, Director of National Security and Law Enforcement Liaison at BlackBerry, swore in an affidavit that if the court ordered the RCMP to hand over details about the encryption key, or the key itself, in its possession, it would 'potentially impact relationships with other end-users and law enforcement criminal investigations globally for all foreign countries that BlackBerry operates and provides communication services.'
>
> During the hearings, Crown attorney Robert Rouleau asked RCMP Inspector Mark Flynn: would the disclosure of this information about the global key jeopardize ongoing investigations? 'We have several investigations ongoing right now, varying from individual homicides, organized crime homicides and organized crime and drug investigations occurring in various locations in Canada today [where] our capabilities in this environment are a significant factor,' Flynn said, according to a 2015 transcript filed with the court.[30]

The public impact of privately owned technologies

Big Tech became more central in the national security business through a multi-layered strategy. They did not limit themselves to creating technologies and dictating how governments and users were supposed to use them. They also took over, in a more subtle way, the Internet. Contrary to the widely held view, the Internet and its associated technologies are neither 'neutral' nor 'transnational.' The physical infrastructure (cables, cell masts, satellites, data centres, platforms, etc.) belongs to the private sector. Amazon Web Services, Cloudflare, Microsoft Azure, and Google host the infrastructures of the biggest companies in the world and are deployed in the data centres of national telecom companies and ISPs. A ruler might own the power to activate the kill-switch, but actual power is in the hands of a limited number of Big Tech companies which can act faster than any government.

30 Justin Ling and Jordan Pearson, 'Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key.' *Vice News* 14 April 2016. https://www.vice.com/en/article/kz9kaa/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how (visited 23 February 2021).

Many trust the grassroots nature of Internet governance as a bulwark against public and private intrusion. As soon as the protocols that run the Internet are 'free' there is no way for the powers-that-be to extinguish its freedom. A global Internet shutdown for political or State (self)defence would be mitigated by building another one, using low-tech solutions like solar-powered Wi-Fi mesh networks. The Internet is made of 'protocols' and standards. Protocols are the digital Esperanto that allows computers running different operating systems to exchange data. This Esperanto is in the public domain. Nobody can claim intellectual or industrial property rights. Standards are set by the Internet Engineering Task Force's 'large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.'[31] Also the 'ownership' of the IP numbers (the 'number plates' of Internet-connected computers) and of the domain name system (the scheme to convert IP numbers into letters, thus making easier to remember Internet addresses) and the root servers accreditation (the authority that manages the top global list of Internet domains) is still firmly in the hands of the Internet Corporation for Assigning Name and Numbers (ICANN) and its ancillary organisations. Despite its name, ICANN is an NGO, and is incorporated under and must abide by US law. Over the years it has extended its membership as well as its governance to greater international participation. However, industry and governments have an important presence on ICANN's governing and technical bodies. They do not 'control' ICANN in the same way that they do not control the IETF, but they can of course influence its decisions more than civil society constituencies (and non-US governments) do.

> Microsoft as a whole has been a technical leader in IETF standards activities for decades. Past contributions have benefitted HTTP, IPv6, WebRTC, PPP, PPTP/L2TP, RADIUS & EAP, DNS, iCalendar, WEBDAV, IoT, security, IP mobility, routing and myriad other topics … Other contributions from Windows Core Networking (either directly as editors or working with the main authors and relevant working group) are on topics such as TCP congestion control (DCTCP, CUBIC, LEDBAT++, rLEDBAT), TCP optimizations (TCP Fast Open, RACK, HyStart++), IPv6 (including IPv6 for IoT), WebSockets, and HTTP/2.[32]

31 IETF, 'Who We Are.' 2021, https://www.ietf.org/about/who/ (visited 16 February 2021).

32 Gabriel Montenegro. 'Internet Standards.' *Windows Server Networking Blog* 22 October 2019, https://techcommunity.microsoft.com/t5/networking-blog/core-networking-and-internet-standards/ba-p/924431 (visited 16 February 2021).

The current Internet governance bodies continue to exercise significant efforts to maintain the network on a worldwide scale and ensure its independence. However, as a matter of principle it would make more sense if the network's governance were given, for instance, to the United Nations rather than to a complex architecture of intertwined NGOs and volunteers. It would by no means be a perfect solution, but it would make clear 'who' is doing 'what' and on 'whose' behalf.

The private nature of the technology of information is not an evil in itself, but it is created to pursue private profit rather than satisfy public needs (security, safety, and respect for fundamental rights). As a consequence, many public policy issues related to the extensive availability of communication technologies have been affected by the deliberate choices of US Big Tech regarding how to shape national security and society in general.

There are numerous consequences of this untrammelled dominance. The sale of unreliable software increases the probability of computer-based crimes and attacks on critical infrastructures such as power grids. It often uses the protection of human rights to market products and services or, by contrast, to deny a cooperation request from law enforcement authorities. It also acquires a large volume of data and information about natural and legal persons, and increasingly assumes control over critical sectors of the civil service such as departments of justice and education. These are merely a few examples of how Big Tech pursues profit regardless of its effects on the public interest. Regulators have begun sanctioning these large corporations because of their anti-competitive behaviour, infringement of consumer rights, and their cavalier attitude toward compliance with the provisions relating to personal data protection. Big Tech evinces a high degree of insouciance about such matters. Monetary fines are paid and they carry on 'business as usual.' Their mantra appears to be 'better ask for forgiveness than for permission.'

Policing for the 'greater good'

Dealing with the growing number of digitally fuelled unlawful acts has become increasingly intractable. Crime prevention and criminal investigations tend to be delegated to private bodies such as ISPs and over-the-top platforms. Telecommunication companies and ISPs not only provide the usual warrant-based wiretapping service, they also retain Internet traffic data for, at least in Italy, up to five years to provide long-term access for prosecutors and law enforcement authorities. They have also become an essential component of preventive and sometimes repressive activities. They enforce the removal of online content or the blocking of the activities of certain individuals or groups. That may be to comply with a court order, but it may occur without one. For example, Donald Trump's social media accounts were blocked by the owners of the platforms. This sort of activity continues

on a daily basis, and ordinary users have no means by which to challenge the unilateral enforcement of private 'terms and conditions.' The disruptive effects of these business practices are cultural rather than legal: Big Tech has created an entirely artificial perception of what technology is meant to be.

This pervasiveness does not concern only infrastructure, hardware, and algorithms (see below), but what ought to worry legislators and policy makers are the interfaces. They are the tools that in theory should allow man to control machine, but which in reality enable Big Tech to directly control the thoughts and actions of users, as well as their daily lives. Interfaces have been with us since computers interacted with humans through black screens and green cursors. Because in those early days computers were not widely available, few complained about the oddities of the esoteric rites needed to print the receipt of a bank transaction or a medical prescription. The shift to graphic, mouse-operated interfaces pushed computers from the ivory towers of banks, universities, and various public and private institutions down to ordinary citizens. They had to learn a new language made by gestures: click here first, then there and then drag, and then right-click. They have been brainwashed into a Pavlovian condition in which they do not ask themselves why a certain task must be done in a specific way, why a feature is implemented in a certain manner, or why it exists at all.

The control over interfaces is not just a matter for software architects and 'usability experts.' It is, first, a matter of confining users to a cage of frustration and habit so that once they have processed through the quirks of badly designed interfaces, they remain trapped by them. The cage might be a golden one, however it always remains a cage. This form of control is called 'technological lock-in' and is widely practised in the software manufacturing business to prevent users from switching to competitors' products. However its effects extend well beyond that. Especially in the smartphone-equipped 'thumb-generation,' controlling the interface includes control of behaviour, the exercise of rights, and the application of power. Take the simplest of the messaging apps—a tool widely used also to fuel social disturbance or political protest. Adding, for instance, a button that provides cryptographic features changes its use and purpose. Communicating in such a way that was hitherto impossible provokes social behaviour (not necessarily criminal) that previously would have not even been conceived. By contrast, either denying the availability of a feature or making its function impractical prevents a person from even understanding that he or she may hold—or withdraw—a right.

The control of interfaces is a structural danger to national security and public order because it is an instrument in the hands of a small number of subjects to express a mono-culturalism that reduces our differences to zero. Wherever one happens to be in the world is irrelevant; by using the interfaces of technological instruments hundreds of millions of people behave in the same way because there is only one way in which to use these devices. Interfaces mark the time, rhythm, and frequency of what we do and,

therefore, condition our values. The power of interfaces, however, is not limited to facilitating or denying the availability of a feature or a functionality. It extends to the capability of conveying sense and values by way of their graphic appearance. Graphic interfaces make extensive use of images to deliver messages and impart orders. Graphic interfaces *are* metaphors, and metaphors, as Milton Erickson demonstrated, affect human behaviour unbeknown to the 'patient.'

The alarm—like so many others, unheeded—was raised a long time ago. In an essay published in 1999, Neal Stephenson drew a parallel between the use of metaphors in the world of entertainment and the world of computing.

> Disney and Apple/Microsoft are in the same business: creating a short circuit between complex and explicit verbal communications with interfaces of enormous design costs. Disney is a kind of user interface as such – and not just a graphical one. Let's call it a Sensory Interface. It can be applied to anything in the world, real or imagined, albeit at a staggering cost.
>
> Why do we reject explicit interfaces (words) and rely on graphical or sensory interfaces – which explains, by the way, the success of both Microsoft and Disney)?
>
> The reason, in part, is simply that today's world is very complicated – much more complicated than the hunter-gatherer world our brains evolved to survive in – and we simply cannot handle all the details. We have to delegate. We have no choice but to trust some nameless artist at Disney or programmer at Apple or Microsoft to make some choices for us, close some options and give us a conveniently packaged executive summary. But an even more important consideration comes from the fact that, during this century, intellectualism has failed, and everyone knows it. In places like Russia and Germany, ordinary people have agreed to loosen their grip on their traditions, customs and religion, and leave the ball in the hands of intellectuals. In doing so, they have ruined everything and turned this century into a shambles. Those wordy intellectuals were once just boring; now they seem a bit dangerous too.[33]

The evolution of computer interfaces' design is revealing. Skeuomorphic design—mimicking the aspect and the functioning of physical objects in their

33 Neal Stephenson. 1999. *In the Beginning… Was the Command Line*. New York – USA, William Morrow Paperbacks, Kindle Editions loc. 590–612.

digital replicas—is a widely practised interface design method. Software versions of famous guitar amplifiers or sound processing pieces of equipment carefully replicate the appearance of their analogue ancestors. The same is true of countless examples including slot-machines, keypads, switchboards, and control panels of various types of equipment. In the other corner of the ring is the opposite view: the validity of breaking the connection between physical objects and the way they can be controlled via computer interfaces by 'flat-design' or cartoon-like visuals.

Superficially, skeuomorphic design is no more than a method of simplifying the use and understanding of a specific feature. If an icon is shaped in the form of a screwdriver and a hammer it hints at some 'under the hood' features. Similarly, a red cross-like symbol suggests 'ICE' functionality. On the other hand, flat-design and cartoons provide more room to refine the message (the command, really) and guide the user's behaviour. And this is exactly the point. There are more subtle influences in this kind of interface design pertaining to what has been called the rhetoric of skeuomorphism and—in general—of visually oriented interface design. The ubiquitous and ethically questionable practice of 'nudging' has found its way also into how digital interfaces work:

> Online decision making is almost always influenced by heuristics and biases; consequently, the concept of digital nudging applies not only to online consumers' decision making but also to various other contexts, from e-health systems to social media apps to organizational information systems. Whereas such factors as presenting reviews or highlighting markdowns are well known for having a strong effect on user behavior in general, digital nudges influence decisions at the point and moment of decision making. In particular, digital nudging works by either modifying what is presented—the content of a choice—or how it is presented—the visualization of a choice—as in, say, changing the design of the user interface.[34]

As much as these techniques are enforced to elicit the purchase of goods and services, it is clear that nothing prevents the use of interfaces and their behavioural control-oriented design technique from influencing political and social beliefs, as well as to reduce citizens' critical thinking to an infantile level.[35] An abstract, software-controlled layer divides reality from its perception and, in the case of augmented-reality, it *creates* the perception

34 Christoph Schneider, Markus Weinmann, and Jan vom Brocke, *Digital Nudging: Guiding Online User Choices through Interface Design*. Communications of the ACM, 61:67–73, 2018. 10.1145/3213765 (visited 30 January 2021).

35 Simon Gottshalck, 'The Infantilization of Western Culture.' *Salon* 8 August 2018, https ://www.salon.com/2018/08/08/the-infantilization-of-western-culture_partner/ (visited 23 February 2021).

of the surrounding world. And this is yet another power firmly in the hands of Big Tech. This result would be impossible to achieve without deferring to software the task of searching, analysing, and correlating correlate information. This is where Big Data and artificial intelligence (AI) step in, with their unique selling proposition in regard to crime prevention and national security protection.

National security, AI, and Big Data

It began with the advent of CCTV. Camera-surveillance was thought capable of deterring potential offenders. It actually did not, and turned into an instrument of mass-gathering information to be exploited *ex post* rather than as a pre-emptive or real-time threat management system. Perfectly matching the approach of Internet traffic-data retention, CCTV surveillance feeds are stored and retrieved in case of need such as the identification of the perpetrators of social unrest, crimes, and violence generally. Apart from specific application, where humans are ready to intervene in case of alarm, 'intelligent' surveillance systems are meant to 'stay behind.' CCTV is still the main visual depiction of surveillance.

The race for the ultimate 'prevention' tool has been recently joined by two new competitors: profiling and predictive policing software. These are run by AI which, it is claimed, can make sense out of 'Big Data' collected from every kind of source, from public records to—again—camera feeds, from social networks to behavioural data. These two ubiquitous buzzwords carry a series of ambiguities (the actual meaning of the word 'intelligence,' the pretence that 'Big Data' can provide predictive hints without a social theory of behaviour and crime, the possibility of automating public policing) that directly affect the way we live. Even if automated policing were feasible (and it is not), to make it work we would have to shape our society according to the needs of these technologies. Is this desirable? Are governments actually in control of these systems? And is their enforcement actually subject to *effective* parliamentary oversight?

Notwithstanding these doubts, it goes without saying that a number of private companies have emerged, promising to deliver the best technology to monitor, prevent, investigate, and indict. The limitations of real-time monitoring technologies, including their early form of ubiquitous analogue CCTV systems, have long been revealed. Firstly, it is obvious that, if delegating to software the task of preventing and investigating criminal offences, such software must enforce a social—hence, political—theory of crime. Face-recognition technology is asserted to be up to 90 per cent accurate.[36]

36 Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Proceedings of Machine Learning Research 2018 Con-

However, early studies account for different figures exposing the issue of bias in recognition algorithms developed by IBM and Microsoft.[37]

Moreover, if the platform is supposed to detect a crime in its early stage it must necessarily be instructed to distinguish lawful from unlawful conduct. To interpret a stabbing or a break-in, or their inchoate signals, as potentially criminal behaviour is (relatively) easy. Deciding if a person who approaches another constitutes harassment is more difficult even for the trained human eye of a police officer. Secondly, if they operated flawlessly (and they do not), they would notice 'everything.' Therefore, police would have no excuse not to investigate petty transgressions such as irregular parking and offensive name-calling. Do law enforcement agencies have the power or the courts the time to do this?

In regard to courts, the question is frequently raised whether AI could replace the judge. Could we one day see the *bouche de la loi* idealised by Montesquieu? It would be unhindered by the tedious interventions of counsel, and simply extract the *bare* data from pre-emptive policing platforms, *correlate* them to the defendant's details and personality traits, *design* a theory of the case, and finally, hand down a verdict. Sadly perhaps, this is pure science-fiction. One reason why it is unlikely to occur is that AI is *designed* to err.

To explain this provocative claim, we need a brief digression on the subject of AI. The idea that software can operate better than a human being relies upon the old-fashioned assumption that a computer programme is always right and works faster and more efficiently than a human. This was certainly the case with early deterministic machines and their modern iteration. Programmable logic controllers (PLC) utilised in industry, as well as modern digital firewall rule-based configurations are able to perform numerous tasks, although this is predetermined by the way they are programmed. The evolution of the interaction between a computer programme and the space in which it is immersed was made possible by a huge quantity of sensors, as well as by the increase in computing power that provided the machines with progressively more autonomous functioning. However, they still remained machines unable to make sense out of the action they performed.

This is well explained by the John Searle Chinese Room experiment. Computers function through syntax, not meaning. They behave *as if* they were 'intelligent.' However, they are not. They are, in other words,

ference on Fairness, Accountability, and Transparency, 81:1–15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (visited 24 February 2021).

37 Alex Najibi, 'Discrimination in Face Recognition Technology.' 24 October 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (visited 25 February 2021).

mimicking intelligent behaviour, not consciously adopting it. This imitation game is what enables the proponents of the functionalist approach to call a computer programme 'intelligent.' It works according to the 'duck test': if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck. Or, in a national security context, 'If it looks like a terrorist, if it acts like a terrorist, if it walks like a terrorist, if it fights like a terrorist, it is almost certainly a terrorist.'[38]

Imitating the way humans behave is a reasonable approach by which machines can serve us and, as the promise of technology always asserts, free mankind from menial tasks. But this is not an accurate representation of reality. Negative consequences of the functionalist approach have been augmented by a shift in the use of language to describe the way (digital) machines work. When computer programmes reached a level of (moderate) autonomy as humans, the word 'functioning' was replaced by the word 'behaviour.' The different semantic weight of the two words should not be underestimated. 'Functioning' belongs to the realm of machines, 'behaviour' to the world of humans. If a machine has a 'behaviour', this is the next logical step to claiming that it is also 'intelligent.'

Artificially intelligent

This conclusion was supported by so many widely reported claims that even AI experts could not understand what the software was doing. The deduction goes: I created the software, I cannot explain why the software provides an outcome, and therefore the software is 'intelligent.' This reasoning, however, is flawed by a fallacy of ignorance. Being unable to explain how a magician produces his trick does not imply that he is violating the laws of nature. It only means that the audience is unable to spot his chicanery. In the same way, the fact that a non-technical person cannot explain (or understand) how a computer programme could 'behave intelligently' does not means that the software 'is' intelligent. Once again, the point is that to exhibit autonomous operating capabilities may not be equated to 'intelligent.'

Even the respected *MIT Technology Review* falls into this trap:

> No one really knows how the most advanced algorithms do what they do. That could be a problem … There's already an argument that being able to interrogate an AI system about how it reached

38 Don Melvin, Susannah Cullinane, and Mohammed Tawfeeq, 'Russia's Lavrov on Syria targets: "If It Looks Like a Terrorist, Walks Like a Terrorist …"' *CNN Middle East* 1 October 2015, https://edition.cnn.com/2015/10/01/middleeast/russia-syria/ (visited 24 February 2021).

> its conclusions is a fundamental legal right. Starting in the summer of 2018, the European Union may require that companies be able to give users an explanation for decisions that automated systems reach. This might be impossible, even for systems that seem relatively simple on the surface, such as the apps and websites that use deep learning to serve ads or recommend songs. The computers that run those services have programmed themselves, and they have done it in ways we cannot understand. Even the engineers who build these apps cannot fully explain their behavior.[39]

When we stop to analyse the matter it is evident that an algorithm is a series of abstract steps. Pythagoras' theorem is an algorithm. What puts an algorithm to work is its implementation, or, in other words, its 'embedding' into a computer programme (or, in general, the attribution of specific tasks to humans, machine, or a combination of the two). A computer programme, interacting with the environment through sensors and/or parsing Big Data can provide outputs in a non-deterministic way. To operate in this way, the computer programme must be tuned by loading data of various kinds and sources. Once the software has processed the correct amount of data, it starts providing outputs. The more carefully selected the training data, the better the software will operate. That explains why Big Data (or better 'Big *Raw* Data') are crucial; they allow the tuning of algorithms and implementations. But that neither implies that they have become 'sentient' nor that they are 'intelligent.' Moreover, uncertainty about how 'AI,' machine learning, and neural networks (the 'Holy Triad' of computer data management) work is intrinsic to the theories upon which they have been built. It is an attempt to turn the deterministic output of a computer programme into something that can better adapt to environmental circumstances—such as autonomous driving—where all elements of the software's functioning cannot be predetermined. The price for setting software free from determinism is factoring the possibility of error and mistakes into the output. From a strictly legal perspective, it is irrelevant if the designer, the programmer, or the operator is not capable of foreseeing the reactions of the machine they have built or made work. They are and remain the sole and only responsible (and liable) persons for the incidents and accidents caused by their product.

These, and other questions relating to racial profiling, have been raised to the next level by the inescapable evolution of visual surveillance (face recognition), data-aggregation platforms, and profiling software. The synergy between these products promises to solve the problem that plagues

39 Will Knight, 'The Dark Secret at the Heart of AI.' *MIT Technology Review* 11 April 2017, https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ (visited 25 February 2021).

national security and law enforcement agencies: information overload triggered by the availability of huge quantities of data and the limited ability to correlate them. The capability to influence human behaviour revealed by the synergy between the Jungian-inspired Big Five Personality Traits and a Skinner-powered feedback system is too attractive to governments and corporations. As private companies providing 'AI-powered,' Big Data-fed proprietary platforms are now occupying this profitable market niche, this is not only a question about respect for fundamental rights and due process. It directly affects the role of private companies in influencing or shaping the response to an attack or event, crime-fighting, and national security policies.

The description of how a crime monitoring and prevention (demo) platform is supposed to work is self-explanatory:

> The screen displayed a map of the East Side of Chicago. Around the edges were thumbnail-size video streams from neighborhood CCTV cameras. In one feed, a woman appeared to be unloading luggage from a car to the sidewalk. An alert popped up above her head: 'ILLEGAL PARKING'. The map itself was scattered with color-coded icons—a house on fire, a gun, a pair of wrestling stick figures—each of which, Gaccione explained, corresponded to an unfolding emergency. He selected the stick figures, which denoted an assault, and a readout appeared onscreen with a few scant details drawn from the 911 dispatch center. At the bottom was a button marked 'INVESTIGATE,' just begging to be clicked.[40]

The very same approach (delegating to private entities the building of a decision-making platform fed by public information) was endorsed by the British government during the COVID-19 pandemic. It provides another instructive example of the public-private entanglement caused by Big Tech sovereignty over the technology of information:

> On 28 March 2020 the British Government announced its strategy to use various technologies 'for coordinating the response with secure, reliable, and timely data—in a way that protects the privacy of our citizens—in order to make informed, effective decisions' … In respect of the private sector's involvement, five companies were selected. These were Microsoft to provide support to store the data sources in its data centres, Amazon Web Services (if the convoluted writing has been correctly interpreted) to be used to make

40 Arthur Holland Michel, 'There Are Spying Eyes Everywhere—and Now They Share a Brain.' *Wired.com* 2 April 2021, https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/ (visited 26 February 2021).

> the platforms work, Google to collect real-time information on hospitals' response, Palantir Technologies UK to enable 'disparate data to be integrated, cleaned, and harmonized in order to develop the single source of truth that will support decision-making', and, finally, Faculty to carry out the development and execution of the data response strategy. This includes developing dashboards, models and simulations to provide key central government decision-makers with a deeper level of information about the current and future coronavirus situation to help inform the response.[41]

The promise of making sense out of the chaos of unrelated, non-standardised, inaccurate data in order to obtain useful information and manipulate reality with just a few keystrokes or mouse clicks is too seductive to be resisted. It also explains why Big Tech is so advanced in this form of research: collecting data about the daily behaviour of billions of users by way of social networking, content-sharing, streaming, and messaging platforms. They are in a position that no government can even dream of. They can submit users' behaviour control to huge software architecture. 'Personalised marketing' benefits from identifying an individual so as to target him or her for various purposes. However, from a broader perspective, personal identity—hence privacy—is not that relevant. What matters is that the *right message* hits the *right target* and the *right target* reacts in the *right way*, for better or worse. AI carries an intrinsic capability to err. Error may be amplified by deliberate choices, introducing biases of various kinds such as targeting ethnicity, political creeds, or—on an international scale—shaping the attitudes of a country. Hence, a fundamental question arises: who guarantees the control over the bias in input and the fixing of the bias in the output?

As in the case of the pretence of reviewing the source code of computer programmes to keep them unaffected by vulnerabilities, the complexity of AI-based infrastructure denies the possibility of effective vetting in respect of bias and acceptable error rates. It affects the ability to prevent indiscriminate tracking or, by contrast, targeting specific social categories to provide (or deny) public services. This will be explained in the next chapter. For the moment, it suffices to say that the answer is political rather than legal and is related to how much *control* a State is ready to relinquish in favour of private entities.

Cyberwarfare and digital mercenaries

Another sector where Big Tech plays an essential role is in supporting States waging under-the-radar wars through digital mercenaries by resorting to

41 Monti and Wacks 2020.

private means and facilities. They soon discovered that 'cyberwarfare' is a convenient way to settle international disputes with acknowledged foes, temporary allies, and unruly partners. Cyberwarfare also benefits from the much sought-after techniques of the contemporary game of propaganda: fear, uncertainty, and doubt about the actual nature and extent of digitally fought battles. US allegations against Russia[42] and China[43] of attempting to influence the 2016 and 2020 American elections and manipulating public opinion might perhaps be supported by solid classified evidence. From a public opinion perspective, though, these claims have not been proved. The US launched their accusations; Russia, while publicly denying them, did nothing to prevent public opinion from expressing concern about its technical and propaganda skills.

Cyberwarfare happens silently, swiftly, and surreptitiously. There are no boots on the ground. No coffins wrapped in the national flag returning back from the front. No media coverage exposing human rights abuse and war crimes. No protests against the government. By contrast, politicians can call for 'cyber strikes' against sovereign countries without fear of being accused of supporting an act of war. Ordering an air strike, the deployment of a military expeditionary contingent, or a special forces intervention is much more complicated than unobtrusively ordering the shutting down of a nuclear plant.

The case of the 2010 *Stuxnet* computer virus that was suspected of being deliberately deployed to damage the Iranian nuclear programme[44] is exemplary. No 'smoking gun' in the hands of the 'usual suspects' was found, and 'plausible deniability' is easy to claim. Whoever the perpetrator may have been, the attack was possible because of the *private* technologies deployed in the Iranian facilities: Microsoft Windows operating systems. The malware exploited zero-day vulnerabilities affecting the operating system to take control of the software controlling the PLC devices used in the plants. There is no evidence that Microsoft supported the operation or that it was aware of it. But a vulnerability of Big Tech allowed officially unknown actors to target a sovereign State. Moreover, the attack seems to have been carried on

42 Niu, Isabelle, Bracken, Kassie, and Eaton, Alexandra, 'Russia Created an Election Disinformation Playbook. Here's How Americans Evolved It.' *The New York Times* 25 October 2020, https://www.nytimes.com/2020/10/25/video/russia-us-election-disinformation.html (visited 24 February 2021).

43 Reuters, 'China targeting U.S. Election Infrastructure with Cyberattacks, Says O'Brien.' 9 August 2020, https://www.reuters.com/article/us-usa-election-interference-idUSKCN2550Q2 (visited 25 February 2021).

44 David Kushner, 'The Real Story of Stuxnet.' *IEEE Spectrum* 26 February 2016, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (visited 26 February 2021).

by—or with the support of—a mysterious entity called 'Equation Group' with alleged ties to the US national security community.[45]

While the group is believed to have covertly carried out State-sponsored attacks, cyberwarfare has its public side in the form of legitimate security companies providing malware technologies 'to fight terrorism and catch criminals.' As in the private military sector, more than a few cybersecurity companies are run by former(?) members of the military/intelligence community. Moreover, they routinely hire their comrades and remain in touch with their former professional environment. They may also employ individuals with considerable hacking skills and a questionable past. As in the case of PMCs, the involvement of private entities in the national cybersecurity field may come in handy when the State does not have the resources (or the time) to develop on its own a digital warfare/intelligence platform or when official bodies cannot be involved in retaliation or direct action against a foe.

Of course cybersecurity is a legitimate business and not every provider of such services—or every cybersecurity manager working for Big Tech or a telecom company—is automatically connected to 'grey' or 'black' operations. However, the way the security consultancy business works can easily conceal uncomfortable truths in plain sight.

The cybersecurity business has evolved. In the beginning, vulnerability assessment and penetration tests were executed mainly by human operators, without automated tools. An individual or a small group would probe the robustness of a network infrastructure and try to 'sneak in' using the whole arsenal of a hacker, from social engineering to systems' misconfiguration and software defects. Modern cybersecurity activities involve the deployment of multi-man teams to perform 'Red Teaming' attacks and 'offensive security.' These two key concepts are essential in understanding the role that a security company can play in national security operations. Adapted from the military realm, Red Teaming is a no-holds-barred attack on an infrastructure. To the Red Team, everything and everybody is a potential target in achieving the final result: penetrating (or impairing) a network. The legal status of Red Teaming is not entirely clear. Attacking an infrastructure can be done with the authorisation of its owner. Targeting individual employees by feeding them with computer viruses, false emails, or other malware may not be covered by the initial agreement with the employer. Similar concerns affect the 'offensive security' model. Based on the old adage that 'attack is the best form of defence,' the offensive security model endorses the use of

45 Dan Goodin, 'How "Omnipotent" Hackers Tied to NSA Hid for 14 Years—and Were Found at Last.' *Ars Technica Biz&IT* 16 February 2015, https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/ (visited 24 February 2021).

active measures to respond to an attack. In other words, when attacked, fight back. Proponents of this model are careful in pointing out that offensive security may easily cross the line and become a criminal offence in itself. However, setting the legal threshold not to be crossed is not easy, as it is difficult to see it in the middle of an attack.

Red Teaming and offensive security can become a powerful instrument to protect national security. However, and once again, there is a price to be paid. If the State is incapable of deploying technology to pursue its goals, the inevitable consequence is the involvement of cybersecurity 'contractors' whose role might become hard to distinguish from that of mercenaries. There is one difference: the role and the operating procedures of traditional military contractors are known and, therefore, relatively easy to monitor and control. The cybersecurity contractors, by contrast, are ghosts in plain sight. Very few in the public sector understand what these often-shady characters do, or how.

International scandals like the Hacking Team case demonstrate the dangers arising from the blind involvement of private entities in the public policy and national security realm.[46] It also reveals the contradictory attitude of governments, ready to 'dump' a private partner as soon as its presence becomes embarrassing. As one of the few cases that become public on the international stage, it deserves a closer examination. The malware platform Remote Control System, created by Hacking Team, was software capable of covertly sneaking into the targeted computer opening a communication channel with its 'master.' It was able to monitor the behaviour of computer users, as well to 'exfiltrate' contents and, by contrast, to upload *ad hoc* manufactured information, take control of the device's microphone and camera. Its existence became public in 2016 when a leak online disclosed the list of private and institutional clients of the company and the computer code of the platforms. The potential for abuse of this computer programme is huge. Something should have been done to prevent the illegal use of this piece of software. The company, apparently, took the matter in hand:

> The Hacking Team's existing customer policy – posted on its website one year after Citizen Lab exposed the Italian firm – vows to sell only to governments, not to corporations or individuals … Yet it will not, under any circumstances, sell to a country blacklisted by the United States, European Union, United Nations, NATO, or the Association of Southeast Asian Nations. To help Vincenzetti

46 The Italian company providing offensive security services has been selling its Trojan horse not only to Western intelligence and law enforcement agencies, but also to non-democratic regimes.

> review clients in advance of sales, he says he hired Bird & Bird, an international law firm headquartered in London.
>
> Though the Hacking Team does not track how clients use RCS after a sale, Vincenzetti says he does monitor the media to ensure clients do not commit crimes. 'Should questions be raised about the possible abuse of HT software in human rights cases,' the company states in its customer policy, 'HT will investigate to determine the facts to the extent possible. If we believe one of our customers may be involved in an abuse of HT software, we will contact the customer as part of this investigation. Based on the results of such an investigation, HT will take appropriate action.'[47]

Later analysis of the leaked information revealed that RCS had actually been used to run operations against political opponents of regimes, as well as journalists. This engendered protests, but they overlooked the core of the matter: the operational latitude given to the company and the importance of the rule of law in every country that purchased this piece of software.

Notwithstanding the critical nature of this platform, the governments of the (liberal) countries who purchased RCS accepted the 'scrutiny' of their supplier, at least on paper. Hacking Team claimed to monitor the use of its platform and 'take action' in case of abuse. In truth its customers used RCS at their own risk, according to the latitude allowed by specific laws of the various jurisdictions. This is a crucial point. An offensive security digital platform has been sold—it goes without saying—to Italy, and in compliance with export control regulation to States that were allowed to purchase it (including the US, South Korea, Spain, Denmark, Thailand, Mexico, and other UN member countries). While the existence of RCS was kept confidential, especially in law enforcement circles, this was fine. But when the news about RCS broke thanks to a leak, the usual tide of outrage occurred in the media and online. Oddly enough, it was Hacking Team that took the blame rather than the governments that abused the tools.

What happened to Hacking Team is neither the first nor will it be the last time a (cyber)security company that lives by the sword dies by the sword. It is interesting, though, to analyse the criticism of Hacking Team's platform and the company itself. Hacking Team has been accused of being 'unethical' because of the sale of its products to countries that do not respect human rights. In particular, so the criticism goes, there are suggestions that Hacking Team's malware was exploited to plant fake evidence in the targeted computers. Planting fake evidence is a disturbing practice well-known among

47 David Kushner, 'Fear this Man.' *Foreign Policy* 26 April 2016, https://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/ (visited 24 February 2021).

the law and law enforcement fraternity. In the case of intelligence operations, blackmailing is a standard tool-of-the-trade, and how it is executed is irrelevant. Violations of the rules of evidence or borderline activities in the grey zone are a legal and political liability of those in charge and who decide to cross the line. By contrast, a company is simply supposed to be legally compliant and ethically responsible. As soon a State has a seat in the UN, and the sale respects international laws and treaties (such as the Wassenaar Agreement), doing business with such countries does not raise any eyebrows. Nonetheless, the Italian authorities revoked *ex post* the technology export licence. The official reason was motivated by the discovery that RCS has been *used* to infringe human rights in democratic countries. There is a difference, not taken into consideration by the Italian authorities, between a legal sale of dangerous products and autonomously exploited by the customer in violation of its national laws, on the one hand, and selling the product unlawfully. Notwithstanding that Hacking Team fell into the first case, it was held responsible for somebody else's behaviour. In the second case, the company would have been directly liable for infringing export regulations. Dumping a contractor because of the public outcry generated by its existence is the demonstration of the frailty of governments in relation to the digital side of national security.

Another accusation against Hacking Team was that, because of the leak that revealed the existence of RCS, the company had jeopardised investigations and covert activities around the world. Actually, though, the investigations were jeopardised by governments' choice of resorting to a private contractor instead of developing in-house intelligence-gathering tools. Moreover, law enforcement and intelligence operations have been affected by the lack of contingency plans in the event that things went wrong, as happened. Faith in, or delegating responsibility to, a private contractor to exploit plausible deniability has its drawbacks.

On the technical side, concerns have been expressed about the dangers caused by the public availability of RCS. The possibility has been suggested of a 'black' Hacking Team's software clone that would threaten the national security. RCS malware is far from being the only breed of this kind of software. The Internet is replete with brilliant (rogue) programmers who can build RCS-like software.

Another anxiety is that Hacking Teams' software was untraceable and that it could and would be used without control. RCS was able to exploit the vulnerabilities (i.e. the errors made in the design, writing, and implementation) of popular operating systems and computer programmes (that returns us to the vexed subject of the liability of Big Tech and software manufacturers in particular). This does not, however, mean that the RCS malware was invincible, and while it could fly under the antivirus radar, it does not follow that there is no defence. Even adopting minimal precautions based on digital hygiene (using emails in plain-text, refraining from clicking

on whatever blinks on the screen, looking for network traffic generated by a device, using encryption, and storing passwords carefully) can reduce the effectiveness of such malware.

The outrage generated by the existence and the (sometimes cavalier) use of RCS, though, did not prevent governments from continuing to use RCS-*like* computer programmes. Since 2015 Italian public prosecutors have used *captatori informatici*—a fancy, politically correct synonym for State malware—whose role was eventually sanctioned in 2020 by amending Article 266 of the Italian criminal procedure code. It is unknown whether the malware operated by Italian prosecutors is manufactured by the civil service or—once again—provided by a third party. It is public knowledge, by contrast, that the German Ministry of Interior developed its own Trojan (the *Bundestrojaner*) and planned to use a private-sector manufactured spying tool[48] apparently without legislative authority. It has used it as a wiretapping tool since 2011.[49] US law enforcement is known to employ similar malware since at least 2015 and simpler versions since 1999.[50] State-operated malware is no longer an evil.

Hacking Team and Equation Group are two faces of the same coin. They do the same thing: they make available to State actors technologies and resources that a government cannot (economically and/or politically) afford. But there is a difference; Hacking Team (and its like) build tools to enforce national security and law enforcement goals. Equation Group-like entities *are* the tools to reach it. They are both necessary in a scenario where conflicts are asymmetric, law is progressively difficult to enforce, and the powers-that-be need to defend themselves from criticism, protests, and coups. They also demonstrate that the lack of clarity in the national security/public order legal framework exposes both State and citizen to the unforeseeable blows of political expediency.

48 Falk Steiner, 'Neuer Bundestrojaner kurz vor Genehmigung.' *Deutshclandfunk* 22 February 2016, https://www.deutschlandfunk.de/software-fuer-bundeskriminalamt-neuer-bundestrojaner-kurz.1773.de.html?dram:article_id=346293 (visited on 24 February 2021).

49 Zeljka Zorz, 'Government Telecommunication-Spying Malware Opens Backdoor.' *Helpnet Security* 10 October 2011, https://www.helpnetsecurity.com/2011/10/10/government-telecommunication-spying-malware-opens-backdoor/ (visited 25 February 2021).

50 Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*. William&Mary Bill of Rights Journal, 26(2): 311, 2017, https://scholarship.law.wm.edu/wmborj/vol26/iss2/4 (visited 24 February 2021).

6

CONCLUSION

Whither national security?

National security is no longer controlled by governments. It is shared with the private sector. This often engenders tension between their respective objectives and hence strategies.

Policing-by-data is now the universal mantra. But this has led to misplaced faith in policing-by-*Big Data* and, as we have attempted to show, the irrational belief that eventually the prevention, detection, and prosecution of crime may be delegated to an 'intelligent' computer platform. Cyberspace, William Gibson's 40-year-old fictional creation, has been taken for real. It has been given a legal status and a political role. It has shaped the regulation of national (cyber)security. This confusion is now afflicting the attitude towards robotics and artificial intelligence (AI):

> Robotics and AI may de-responsibilize people whenever an autonomous system could be blamed for a failure. A recent EU proposal to treat forms of AI as 'electronic persons'[1] would only exacerbate this problem.[2]

Ever since the initial, crude versions of these technologies, it is evident that they affect democratic systems more subtly than this: they shape them not according to the 'will' of software but to the business strategies of private companies that created them. The leverage over national security is changing hands.

The private sector has, of course, long been involved in these matters either because the State lacked the appropriate capability or merely for its convenience. What is different now is the manifest loss of governance over the decision process, and policy makers' reduced analytical skills on a more

1 EU Parliament, 'Motion for a European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics.' 2017, https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html?redirect (visited 26 February 2021).

2 Floridi, Taddeo et al. 2018: 11.

DOI: 10.4324/9780367809775-6

structural scale. The delusion is that it is possible to privatise the functions of national security and, at the same time, maintain control of strategy. Whoever controls the functions defines the strategy, and the private sector creates those functions. A useful analogy is the efficacy of the 'like' function on many platforms. Clicking 'like' expresses a direct black-or-white opinion.

This simple device has built an entire (profitable) ecosystem that has affected the approaches adopted towards marketing, advertising, the media, politics, and policymaking.

The power of Big Tech has not yet succeeded in reducing the effective operation of governments and legislatures. This could occur when countries are formulating their long-term industrial, financial, or environmental plans. It might magnify emergencies where there is no time to think. There is a strong temptation to accept suggestions emanating from AI at face value. Trusting computer-generated outputs without careful critical examination is tantamount to relinquishing the human capacity to act semantically—making sense of reality—in favour of a blind, syntax-ruled process where conclusions are drawn from merely following the rules and ignoring any black swans. This inexorably fosters the self-serving justification, 'I merely obeyed orders' or, in this context, 'We followed the rules laid down by whoever created the computer programme.'

On the other hand, the immateriality and the de facto social acceptance of pervasive surveillance, behaviour controls, and the adoption of direct, non-court-mediated measures to settle in-platform disputes and claims have reduced sensitivity to Big Tech's march on political decision-making. The EU Commission has relentlessly called for Big Tech to pull the chestnuts out of the fire on its behalf in respect of a number of critical matters, from Internet traffic data retention to blocking disinformation and protecting critical infrastructures. It has effectively admitted its failure to protect fundamental rights and the security of the Union.

Committing hostile acts against sovereign countries without a formal war declaration, allowing homeland security to stop and question every citizen at will, covertly nudging them rather than assuming full political responsibility for public policy might once have sparked protests, even civil disorder. But these activities are now considered, by the governments themselves, commonplace. There is no need to follow the rules. What matters is the result. Originally, democracy was a *delegation* of power from the citizen to the State. However, the current situation represents a disquieting *transfer* of power from citizen to government, and then to the masters of the technology of information. It is eroding the contrast between liberal democracies and authoritarian regimes.

Historically, national security has protected rulers rather than citizens. This approach was easily applied when rulers' powers were largely untrammelled. Since national security has lain hidden in the twilight zone between politics and law, the shift toward 'lawfare'—the weaponisation of rights—is unstoppable. It is the reason why, and this is the principal message of this book, national security should be given proper legal status. It should be taken out of the dark and balanced against other elements of the public interest and individual rights.

A possible normative definition of national security might include the protection and prevention of internal and/or external actions, activities, or events that harm directly and/or endanger national interests in the economic, scientific, technological, and political fields, without prejudice to the functions of the military in defending the State and those responsible for 'homeland security.' Whether such a proposal is feasible, however, is not a simple question. The reality of *machtpolitik* might dictate that other considerations enter the picture—especially the enormous influence of the international Titans on the world.

Technology-enhanced anarchism has turbocharged the proliferation of offline and online protests, disturbances, and riots. Not only are people accustomed to social networking, instant messaging, and content sharing tools to organise protests and propaganda. At a deeper and substantive level, they have turned technology against their governments. They have created alternative monetary systems in the form of cryptocurrencies, and undermined the financial mechanisms of the stock exchange. They have, in effect, built a 'parallel world' where no State actor is supposed to have access. They have 'industrialised' the flow of leaks relating to State secrets.

This is not, however, a binary confrontation of powers. We are not facing a re-enactment of the traditional conflict between people and rulers. More than ever, Big Tech, the masters of the technology of information, is another player with which to be reckoned. They run—and own—all physical and logical infrastructures that make our world function. They control the lives of individuals and countries by their control over information. Being multinational, they no longer have an allegiance to a specific State or values. They operate their own agenda.

There is no simple solution to this technological takeover. Nationalisation of the technology of information is out of the question. We need instead to find a different approach to the protection of both democracy and national security. This must done, first, by changing the conception of national security. It can no longer be perceived as protection of government from the people. The opposite ought to be the case. National security must become a recognised part of the legal system, and shed its political garb. This would

facilitate a more transparent equilibrium between the public interest and individual rights and, at the same time, it could contribute to the formation of a legal fortress from which to challenge the superpowers of the private sector.

Until this happens, national security will remain, for governments, a shortcut and a justification to enter into a *pactum sceleris* with the masters of the technology of information. And no court would be able to nullify that precarious pact.

REFERENCES

Adams, Alexander. 1835. *Roman Antiquities: Or An Account of the Manners and Customs of the Romans*. Glasgow: Blackie & Son.

Allan, TRS. 2001. *Constitutional Justice: A Liberal Theory of the Rule of Law*. Oxford: Oxford University Press.

Ancarani, Angelo. 1844. *Discorso di Sua Eminenza il sig. cardinale patriarca di Venezia letto nella Chiesa di S. Lorenzo M. il di primo di Ottobre 1843 nell'occasione che vi fu solennemente ristabilito l'inclito Ordine dei PP. Predicatori*. Venice: Antonelli.

Andrews, Christopher, Mitrokhin, and Vasili. 1999. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books.

Arendt, Hannah. 1958. *The Origins of Totalitarianism*. Harmondsworth: Penguin Classics, reprint edition, 2017.

Austin, John. 1832. *The Province of Jurisprudence Determined*. London: John Murray.

Babington, Anthony. 2015. *Military Intervention in Britain: From the Gordon Riots to the Gibraltar Incident*. London: Routledge, Kindle Edition.

Bamford, James. 2021. The NSA and Me. *The Intercept*, 2 October (Visited 14 January 2021).

Ben-Atar, Doron. 2008. *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*. New Haven, CT: Yale University Press.

Bernays, Edward. 1928. *Propaganda*. New York: Horace Liveright Inc.

Bernier, Jean Baptiste. 1929. Droit public and Ordre public. *Transactions of the Grotius Society* Vol. 15, *Problems of Peace and War, Papers Read before the Society in the Year 1929*. Cambridge: Cambridge University Press.

Berzins, Chris and Cullen, Patrick. 2003. Terrorism and neo-medievalism. *Civil Wars*, 6(2), 8–32.

Bingham, Tom. 2010. *The Rule of Law*. Harmondsworth: Penguin.

Blakeley, Ruth and Sam Raphael. 2017. British torture in the 'war on terror'. *European Journal of International Relations*, 23(2), 243–266. https://doi.org/10.1177%2F1354066116653455 (Visited 9 January 2021).

Bobbitt, Philip. 2018. *Terror and Consent*. London: Penguin.

Borisov, Nikita, Ian Goldberg, and Eric Brewer. 2004. Off-the-record communication, or, why not to use PGP. *Proceedings of the 2004 ACM Workshop on Privacy in*

the Electronic Society (WPES '04). Association for Computing Machinery, New York. https://doi.org/10.1145/1029179.1029200 (Visited 25 January 2021).
Breccia, Gastone. 2019. *L'arte della sopravvivenza. Intelligence e sicurezza nell'Impero romano d'Oriente*. Rome: Nuova Argos.
Burke, Bernard. 1881. *The Book of Precedence*. London: Harrison.
Burkert, Walter. 1972. *Lore and Science in Ancient Pythagoreanism*. Cambridge, MA: Harvard University Press.
Cancès, Claude. 2019. *Histoire du 36 quai des Orfèvres*. Paris: Mareuil Éditions.
Catanzariti, Mariavittoria. 2004. *Segreto e potere. I limiti della democrazia*. Turin: Giappichelli.
Centola, Donato. 2016. L'accusa nel sistema processuale delle quaestiones perpetuae tra funzione civica, dimensione premiale e disciplina sanzionatoria. In Solidoro, Laura (ed) *Regole e garanzie nel processo criminale romano*. Torino: Giappichelli.
Channing, Iain. 2015. *The Police and the Expansion of Public Order Law in Britain, 1829–2014*. SOLON Explorations in Crime and Criminal Justice Histories. London: Routledge.
Chao, D. 1988. Despotism in Ancient China. A comparative study of the political thought of Confucius and Montesquieu. *Indian Journal of Political Science*, 49(2), 175–189. http://www.jstor.org/stable/41855365.
Chen, Albert H. Y. 2019. A perfect storm: Hong Kong–Mainland rendition of fugitive offenders. *Hong Kong Law Journal*, 49, 419–429.
Chen, Yongxi. 2016. Transparency versus stability: The new role of Chinese courts in upholding freedom of information. *Tsinghua China Law Review*, 9(1), 79. http://www.tsinghuachinalawreview.org/articles/PDF/TCLR_0901_CHEN.pdf (Visited 30 July 2020).
Cicero *Epistulae ad Brutum* 2,5,1 in Bellincioni, Maria. 1974. Cicerone politico nell'ultimo anno di vita. Turin: Paideia.
Confucius. 2014. *The Analects*. New York: Open Road Media, Kindle Edition.
Cooper, Alan. 1999. *The Inmates Are Running the Asylum*. New York: Macmillan Publishing.
Craig, Paul. 1997. Formal and substantive conceptions of the rule of law: An analytical framework. *Public Law*, 467.
D'Amico, Daniel. 2018. *The Law and Economics of Sycophancy in Constitutional Political Economy*. Springer. https://doi.org/10.1007/s10602-018-9261-6 https://doi.org/10.1007/s10602-018-9261-6 (Visited 18 January 2021).
Dennis, George. 2001. *Maurice's Strategikon: Handbook of Byzantine Military Strategy*. Philadelphia, PA: University of Pennsylvania Press.
Dershowitz, Alan. 1983. *The Best Defense*. New York: Vintage Books.
Dershowitz, Alan. 2003. *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*. New Haven, CT: Yale University Press.
Di Plinio, Giampiero. 2001. La Carta dei diritti nel processo di integrazione europea. In Giuseppe Franco Ferrari (ed). *I diritti fondamentali dopo la carta di Nizza. Il costituzionalismo dei diritti*. Milan: Giuffrè.
Dicey, Albert Venn. 1885. *Introduction to the Study of the Law of the Constitution*. Classic Reprint. London: Forgotten Books, 2012.
Disma, Carlo. 2019. Analisi Strategica. Seminar held at the University of Chieti-Pescara Gabriele d'Annunzio, 22 November.

Doffman, Zak. 2020. Is TikTok seriously dangerous—Do you need to delete it?. *Forbes online edition*, 11 July https://www.forbes.com/sites/zakdoffman/2020/07/11/tiktok-seriously-dangerous-warning-delete-app-trump-ban/ (Visited 20 December 2020).

Donadio, Rachel. 2009. Italy's ex-intelligence chief given 10-year sentence for role in CIA kidnapping. *The New York Times* online edition, 4 November. https://www.nytimes.com/2009/11/05/world/europe/05italy.html (Visited 9 January 2021).

Dondi, Mirco. 2015. *L'eco del boato*. Bari: Laterza.

Donini, Massimo. 2019. Jura et Leges. Perché la legge non esiste senza il diritto. Sistema Penale online edition, 20 December. https://www.sistemapenale.it/pdf_contenuti/1576938432_donini-2019a-iura-leges-non-esiste-legge-senza-diritto-converted.pdf (Visited 15 December 2020).

Dray-Novey, Alison. 1993. Spatial order and police in imperial Beijing. *Journal of Asian Studies*, 52(4), 895.

Dryden, John. 1910. *Plutarch: The Lives of the Noble Grecians and Romans*, trans. by John Dryden and revised by Arthur Hugh Clough. London: Random House.

Dunlap, Charles J. Jr. 2015. Lawfare. In John Norton Moore et al. (eds.) *National Security Law & Policies*. 3rd edition, Durham: Carolina Academic Press.

Duran, Manuel. 2019. Regional diplomacy: A piece in the neo-medieval puzzle?. *BelGeo*, 2(2). https://journals.openedition.org/belgeo/32375 (Visited 20 January 2020).

Dworkin, Ronald. 1986. *Law's Empire*. Cambridge, MA: Harvard University Press.

Dworkin, Ronald. 1978. *Taking Rights Seriously*. London: Duckworth.

Dworkin, Ronald. 1985. *A Matter of Principle*. Cambridge, MA: Harvard University Press.

Dworkin, Ronald. 1985. *A Matter of Principle*. Cambridge, MA: Harvard University Press.

Dworkin, Ronald. 1986. *Law's Empire*. Cambridge, MA: Harvard University Press.

Endicott, TAO. 1999. The impossibility of the rule of law. *Oxford Journal of Legal Studies*, 19(1), 1–18.

Falciani, Hervé Mincuzzi, Angelo. 2015. *La cassaforte degli evasori*. Milano: Chiarelettere.

Feng Zhang. 2015. Confucian foreign policy traditions in Chinese history. *Chinese Journal of International Politics*, 8(2), 197–218. https://doi.org/10.1093/cjip/pov004

Floridi, Taddeo et al. 2018. The grand challenges of science robotics. *Science Robotics*, 3(14), 7, Washington DC: American Association for the Advancement of Science.

Foderaro, Salvatore. 1939. *La Milizia Volontaria e le sue Specialità, Ordinamento Giuridico*. Padua: Casa Edtrice Dott. Antonio Milani.

Fuller, Lon L. 1969. *The Morality of Law*. Rev edition. New Haven and London: Yale University Press.

Furhrmann, Christopher. 2014. *Policing the Roman Empire: Soldiers, Administration, and Public Order*. Oxford: Oxford University Press.

Gall, Lydia. 2020. Ending Hungary's state of emergency won't end authoritarianism. *Human Rights Watch Dispatch*, 29 May. https://www.hrw.org/news/2020/05/29/ending-hungarys-state-emergency-wont-end-authoritarianism (Visited 20 December 2020).

Gardner, Daniel K. 2014. *Confucianism: A Very Short Introduction*. Oxford: Oxford University Press.

Gardner, John. 1994. Rationality and the rule of law in offences against the person. *Cambridge Law Journal*, 53, 502.

Geanakoplos, Deno. 1965. Church and state in the Byzantine Empire: A reconsideration of the problem of Caesaropapism. *Church History*, 34(4), 381–403.

Gellately, Robert. 1991. Rethinking the Nazi terror system: A historiographical analysis. *German Studies Review*, 14(1), 23–38.

Giglio, Vincenzo. 2021. *'L'affaire Shalabayeva' Diritto penale e uomo*. 12 February. https://dirittopenaleuomo.org/wp-content/uploads/2020/01/Giglio_affaire-Shalabayeva-DEF.pdf (Visited 9 January 2021).

Girard, Bonnie. Chinese government-paid scientists plead guilty to stealing research from an American children's hospital. *The Diplomat* online edition, 8 August 2020 https://thediplomat.com/2020/08/chinese-government-paid-scientists-plead-guilty-to-stealing-research-from-an-american-childrens-hospital/ (Visited 12 December 2020).

Gottshalck, Simon. 2018. The infantilization of western vulture. https://www.salon.com/2018/08/08/the-infantilization-of-western-culture_partner/ (Visited 23 February 2021).

Grant, James. 2017. The ideals of the rule of law. *Oxford Journal of Legal Studies*, 37, 383.

Grossman, David. 2009. *On Killing. The Psychological Cost of Learning to Kill in War and Society*. New York: Back Bay.

Guerra, Roberto. 2010. 'I 'Frumentarii' Un dispositivo di allerta e di informazione preventiva nell'antica Roma',*Gnosis.I (3) Rivista Italiana di Intelligence*. Rome: Agenzia Informazioni e Sicurezza Interna.

Guerra, Roberto. 2011. 'Agentes in rebus; agenti in missione' (2) *Gnosis. Rivista Italiana di Intelligence*. Rome: Agenzia Informazioni e Sicurezza Interna.

Haldon, John. 1995. Strategies of defence, problems of security: The Garrisons of Constantinople in the middle Byzantine period. In Cyril Mango and Gilbert and Dagron (eds.) *Constantinople and its Hinterland*. Abingdon: Routledge.

Haley, John Owen. 1991. *Authority without Power: Law and the Japanese Paradox*. New York: Oxford University Press.

Hasic, Anida. 2016. 'Paix et sécurité chez Sénèque : la valeur de la dimension extérieure de la securitas intérieure', *Carmenulae*. Vol. 15. Paris: Sorbonne University. October 2016. http://lettres.sorbonne-universite.fr/IMG/pdf/HasicBat.pdf (Visited 29 August 2019).

Hendley, Katherine. 2009. Rule of law, Russian-style. *Current History*, 108(720), 339. https://media.law.wisc.edu/m/zgyzz/russian_style_rol.pdf (Visited 22 December 2020). https://doi.org/10.1525/curh.2009.108.720.339

Herman, Gabriel. 2006. *Morality and Behaviour in Democratic Athens: A Social History*. Cambridge: Cambridge University Press.

Hobbes, Thomas. 1839–1845. *Opera philosophica, quae latine scripsit, omnia in unum corpus nunc primum collecta studio et labore Gulielmi Molesworth*. London: Bohn.

Hobbes, Thomas. 1839–1845. *The English Works of Thomas Hobbes of Malmesbury*. First Collected and Edited by Sir William Molesworth. London: Bohn, Vol 3.

Holland, Max. 2017. The myth of deep throat. *Politico* online edition 10 September 2017. https://www.politico.com/magazine/story/2017/09/10/watergate-deep-throat-myth-mark-felt-215591 (Visited 21 January 2021).

Hollinger, Richard. 1991. Hackers: Computer heroes or electronic highwaymen? *Computers& Society*, 21(1), 9. June. 10.1145/122246.122248 visited 28 January 2021.

Horatius *Epistole*, I, in Isaia, Arcangelo. 1806. *Delle epistole di Q. Orazio Flacco. Libri due tradotti in verso sdrucciolo*, p. 148. Roma: Antonio Fulgoni.

Horky, Philip. 2016. *Plato and Pythagoreanism*. Oxford: Oxford University Press; Reprint edition.

Hunt, Edwin. 1990. A new look at the dealings of the Bardi and Peruzzi with Edward III. *Journal of Economic History*, 50(1), 149–162.

Hunt, Edwin. 1994. *The Medieval Super-Companies: A Study of the Peruzzi Company of Florence*. Cambridge: Cambridge University Press.

Huntemann, Nina B. and Matthew Thomas Payne (eds.). 2009. *Joystick Soldiers. The Politics of Play in Military Video Games*. Abingdon: Routledge.

Hunter, Virginia. 1994. *Policing Athens: Social Control in the Attic Lawsuits, 420–320 B.C.* Princeton NJ: Princeton University Press.

Irish, John. 2020. Alongside Sisi, Macron says France will sell arms to Egypt irrespective of rights. *Reuters*, *Europe News*. 7 December 2020. https://www.reuters.com/article/us-france-egypt-idUSKBN28H0BG (Visited 22 December 2020).

Jitsuhara T. 2018. Guarantee of the right to freedom of speech in Japan—A Comparison with Doctrines in Germany. In Y. Nakanishi Y (ed) *Contemporary Issues in Human Rights Law*. Singapore: Springer. https://doi.org/10.1007/978-981-10-6129-5_9

Jovičić, Sanja. 2020. COVID-19 restrictions on human rights in the light of the case-law of the European Court of Human Rights. *ERA Forum*, 21, 545–560 (2021). https://doi.org/10.1007/s12027-020-00630-w (Visited 20 December 2020).

Jowell, Jeffrey. 2000. The rule of law today. In J Jowell and D Oliver (eds.), *The Changing Constitution*. 5th edition, Ch 1. Oxford: Oxford University Press.

Khanna, Parag. 2009. The next big thing: Neomedievalism. *Foreign Policy*. https://foreignpolicy.com/2009/09/17/the-next-big-thing-neomedievalism/ (Visited 20 January 2020).

Kramer, Mark. 1999. Declassified materials from CPSU Central Committee plenums. *Cahiers du monde russe*, 40(1–2), 271–306. https://journals.openedition.org/monderusse/pdf/14 (Visited 3 January 2021).

Krisch, Nico. 2012. *Beyond Constitutionalism: The Pluralist Structure of Postnational Law* (Oxford Constitutional Theory). Oxford: Oxford University Press.

Kwoka, Margaret. 2015. Leaking and legitimacy. *UC Davis Law Review*, 48(2) 1400. https://lawreview.law.ucdavis.edu/issues/48/4/Articles/48-4_Kwoka.pdf (Visited 28 January 2021).

Lana, Italo. 1990. *La concezione ciceroniana della pace. in Ciceroniana*. Proceedings of the VII Colloquium Tullianum, Warsaw, 11–14 May 11–14, 1989, Centro di Studi ciceroniani, n.s. VII, Rome.

Lanni, Adriaan. 2016. *Law and Order in Ancient Athens*. Cambridge: Cambridge University Press.

Levy, Steven. 1984. *Hackers, Heroes of the Computer Revolution*. New York: Doubleday.

Linder, Douglas. 2011. The pentagon papers (Daniel Ellsberg) trial: An account. https://www.famous-trials.com/ellsberg/273-home (Visited 24 January 2021).

Lintern, Shawn. 2020. Coronavirus vaccine: Pfizer given protection from legal action by the UK government. *Independent* online edition, 2 December. https://www.independent.co.uk/news/health/coronavirus-pfizer-vaccine-legal-indemnity-safety-ministers-b1765124.html (Visited 12 December 2020).

Luttwak, Edward N. 2009. *The Grand Strategy of the Byzantine Empire*. Cambridge, MA: Harvard University Press.

Luttwak, Edward. 1968. *Coup d'État: A Practical Handbook*. Revised Edition. Cambridge, MA: Harvard University Press.

Mancini, Luigi, et al. 2014. Bypassing Censorship: A Proven Tool against the Recent Internet Censorship in Turkey 2014 IEEE International Symposium on Software Reliability Engineering Workshops, Naples. 389. doi: 10.1109/ISSREW.2014.93.

Markson, Sharri. 2020. Coronavirus NSW: Dossier lays out case against China bat virus program. *The Daily Telegraph* online edition, 4 Maggio. https://www.dailytelegraph.com.au/coronavirus/bombshell-dossier-lays-out-case-against-chinese-bat-virus-program/news-story/55add857058731c9c71c0e96ad17da60 (Visited 15 December 2020).

McCarthy, Kieren. 2020. Here's that hippie, pro-privacy, pro-freedom Apple y'all so love: Hong Kong protest safety app banned from iOS store. *The Register*, Personal Tech. https://www.theregister.com/2019/10/02/apple_hong_kong/ (Visited 12 December 2020).

McCay, Timothy. 1992. *The Crypto Anarchy Manifesto* https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html (Visited 29 January 2021).

McDonald, Jack. 2017. *Ethics, Law and Justifying Targeted*. Abingdon: Routledge.

McFate, Sean. 2015. *The Modern Mercenary*. Oxford: Oxford University Press.

Merlo, Giulia. 2017. Fulvio Croce, l'avvocato delle BR ucciso dalle BR. In *Il Dubbio* online edition. https://ildubbio.news/ildubbio/2017/04/28/fulvio-croce-avvocato-brigate-rosse/ (Visited 15 January 2020).

Miyashita, Hiroshi. 2010. Between 'the Right to Know of the People' and 'Accountability of the Government'. https://www.surugadai.ac.jp/sogo/media/bulletin/Hikaku18/Hikaku.18.103.pdf

Montague, Zack. 2020. Ex-C.I.A. officer sentenced to 19 Years in Chinese Espionage Conspiracy. *The New York Times* online edition. https://www.nytimes.com/2019/11/22/us/politics/jerry-lee-china-spying.html (Visited 12 December 2020).

Monti, Andrea and Raymond Wacks. 2020. *COVID-19 and Public Policy in the Digital Age*. Abingdon: Routledge.

Monti, Andrea. 2018. A contribution to the analysis of the legal status of cryptocurrencies'. *Ragion pratica, Rivista semestrale* 2/2018. Bari:Il Mulino.

Monti, Andrea and Raymond Wacks. 2019. *Protecting Personal Information: The Right to Privacy Reconsidered*. Oxford: Hart Publishing.

Monti, Andrea. 2020a. Critical issues of the Conte-Huawei Decree. *Infosec News* online edition, 24 August 2020. https://www.infosec.news/2020/08/24/news/reti-e-sistemi/le-criticita-del-decreto-conte-huawei/ https://blog.andreamonti.eu/?paged=5&page_id=1218 (Visited 12 December 2020).

Monti, Andrea. 2020b. Dati personali ed esportazione. L'arsenale (giuridico) cinese made. *Occidente in Formiche.net*, 10 December 2020 https://www.ictlex.net/?p=3320 (Visited 22 December 2020).

Monti, Andrea. 2020c. Coronavirus, come funziona la propaganda cinese. *Formiche .net*, 7 May 2020. https://formiche.net/2020/05/covid-19-cina-usa-video-comunicazione/. English translation by Andrea Monti. Available at https://blog.andreamonti.eu/?p=1749 (Visited 20 December 2020).

Moran, Michael, Rein, Martin, and Goodin, Robert. 2008. *The Oxford Handbook of Public Policy (Oxford Handbooks)*. Oxford: Oxford University Press.

Mortati, Costantino. 1940. La costituzione in senso materiale. Milan: Giuffrè.

Nicks, Denver. 2012. *Private. Bradley Manning, Wikileaks and the Biggest Exposure of Official Secrets in American history*. Chicago, IL: Chicago Review Press.

Nippel, Wilfried. 1995. *Public Order in Ancient Rome* (Key Themes in Ancient History). Cambridge: Cambridge University Press.

Orwell, George. 1949. *Nineteen Eighty Four*. Boston, MA: Houghton Mifflin Harcourt.

Palombella, Gianluigi. 2012. *È possibile una legalità globale?: Il Rule of law e la governance del mondo* (Studi e ricerche). Bari, IT: Società editrice il Mulino.

Paramore, Kiri. 2016. *Japanese Confucianism: A Cultural History*. Cambridge: Cambridge University Press Reprint.

Parrott, David. 2012. *The Business of War: Military Enterprise and Military Revolution in Early Modern Europe*. Cambridge: Cambridge University Press.

Peisakhin, Leonid. 2011. Transparency and corruption: Evidence from India. *Journal of Law and Economics*, *55*, 129–149. 10.1086/663727.

Persico, Joseph. 1999. Secrets from the Lubyanka. *The New York Times* online edition, 31 October 1999. https://archive.nytimes.com/www.nytimes.com/books/99/10/31/reviews/991031.31persict.html (Visited 20 January 2021).

Petraccia, Maria Federica. 2014. *Indices e delatores nell'antica*. Roma: Edizioni Universitarie di Lettere Economia Diritto, Milano. https://www.ledonline.it/Erga-Logoi/allegati/701-7-indices-delatores-antica-roma.pdf (Visited 18 January 2020).

Poisson, Philippe. 2019. *15 mars 1667: Création de l'office de Lieutenant de Police de Paris*. https://criminocorpus.hypotheses.org/17397 (Visited 27 August 2019).

Pollman, Mina. 2015. Japan's controversial state secrets law: One year later. *The Diplomat* online edition, 9 December. https://thediplomat.com/2015/12/japans-controversial-state-secrets-law-one-year-later/ (Visited 3 January 2021).

Preto, Paolo. 1994. *I servizi segreti di Venezia*. Milan: Il Saggiatore.

Purpura, Gianfranco. 1979. 'Il "magister officiorum" e la "schola agentum in rebus". *Labeo – Rassegna di Diritto romano*, 25(2), 202–206.

Purpura, Gianfranco. 1985. *Polizia (diritto romano)*. In *Enciclopedia del Diritto*. Vol. 34. Milan: Giuffrè.

Purpura, Gianfranco.1973. 'I curiosi e la Schola agentum in rebus in Annali del Seminario giuridico di Palermo', (XXXIV) Tipografia S. Montaina, Palermo, 165–273.

Raz, Joseph. 1977. The rule of law and its virtue. *Law Quarterly Review*, 93, 195.

Raz, Joseph. 1994. *Ethics in the Public Domain*. Oxford: Oxford University Press.

Raz, Joseph. 2019. The law's own virtue. *Oxford Journal of Leal Studies*, 39, 1.

Redbeard, Ragnar (pseudonym). 1896. *Might is Right or The Survival of the Fittest*. New York: Cornell University Library.

Rowett, Catherine. 2014. The Pythagorean society and politics. In Carl Huffman (ed), *A History of Pythagoreanism*. Cambridge: Cambridge University Press.

Santoro, Raimondo. 2002. *Appio Claudio e la concezione strumentalistica del ius*. In Annali del seminario giuridico della R. università di Palermo. Vol. 47.

Sapori, Armando. 1926. *La crisi delle compagnie mercantili dei Bardi e dei Peruzzi*. Florence: Olschki.

Sbriccoli, Mario. 1998.Vidi communiter observari. L'emersione di un ordine penale pubblico nelle città italiane del secolo XIII. *Quaderni fiorentini*, 27, 231–268.

Schneider, Christoph, Weinmann, Markus, and Brocke. 2018. Digital nudging: Guiding online user choices through interface design. *Communications of the ACM*, 61, 67–73. 10.1145/3213765.

Sciortino, Salvatore. 2011. 'Gli indices nel processo criminale extra ordinem in Atti del convegno 'Il correo narrante fra diritto e storia'. *Iuris Antiqui Historia*. Vol. 3. Pisa, Rome: Fabrizio Serra Editore. http://www1.unipa.it/dipstdir/portale/ARTICOLI%20SCIORTINO/Sciortino,%20Gli%20indices%20nel%20processo%20criminale%20extra%20ordinem.pdf (Visited 19 January 2021).

Seaford, Richard. 2004. *Money and the Early Greek Mind*. Cambridge: Cambridge University Press.

Sharma, P. 2015. *Democracy and Transparency in the Indian State: The Making of the Right to Information Act*. Abingdon: Routledge.

Sheldon, Rose Marie. 2005. *Intelligence Activities in Ancient Rome*. New York: Routledge.

Sheldon, Rose Mary. 2004. *Intelligence Activities in Ancient Rome: Trust in the Gods but Verify (Studies in Intelligence)*. Abingdon: Taylor and Francis.

Shepardson, David, and Reuters. 2020. *Aerospace and Defense*. U.S. adds Chinese drone company DJI to economic blacklist. 18 December 2020 https://www.reuters.com/article/usa-china-drone-idUSKBN28S24I (Visited 22 December 2020).

Sieg, Linda. 2016. Secrecy, hierarchy haunt Japan corporate culture despite Abe's reforms. *Reuters Business News*. https://www.reuters.com/article/us-japan-corporategovernance-idUSKCN0XT222 3 May (Visited 3 January 2021).

Simmonds, Nigel. 2007. *Law as a Moral Idea*. Oxford: Oxford University Press.

Sinnigen, William G. 1961. The Roman secret service. *The Classical Journal* 57(2), 65–72.

Sirrs, Owen. 2011. *The Egyptian Intelligence Service. A History of the Mukhabarat, 1910–2009*. Abingdon: Routledge.

Stephenson, Neal. 1999. *In the Beginning ... was the Command Line*. New York: William Morrow Paperbacks, Kindle Edition.

Tosatti, Giovanna. 1997. 'La repressione del dissenso politico tra l'età liberale e il fascismo. L'organizzazione della polizia' (38)(1) *Studi Storici,* Per il centenario di Jacob Burckhardt Bologna: Fondazione Istituto Gramsci.

Treggiari, Ferdinando. 2011. 'Il bene comune: forme di governo e gerarchie sociali nel basso Medioevo'. *Atti del XLVIII Convegno storico internazionale* Todi, 9–12 ottobre 2011 Spoleto: Fondazione Centro studi sull'Alto Medioevo, 266.

Troeltsch, Ernst. 1915. Der Geist der deutschen kultur. In *Deutschland und der Weltkrieg*. Leipzig: Teubner.

Twiss, S., Chan, J. 2012. The classical Confucian position on the legitimate use of military force. *Journal of Religious Ethics*, 40(3), 447–472. https://doi.org/10.1111/j.1467-9795.2012.00531.x

Volk, Christian 2015. *Arendtian Constitutionalism: Law, Politics and the Order of Freedom*. Oxford: Hart Publishing.

Wacks, Raymond. 1984a. Judges and injustice. *South African Law Journal*, 101, 266.

Wacks, Raymond. 1984b. Judging judges: A brief rejoinder to professor Dugard. *South African Law Journal*, 101, 295.

Wacks, Raymond. 1991. Judges and moral responsibility. In W. Sadurski (ed), *Ethical Dimensions of Legal Theory*. Poznan Studies in the Philosophy of the Sciences and Humanities. Amsterdam: Rodopi.

Wacks, Raymond. 1998. Law's umpire: Judges, truth, and moral accountability. In P. Koller and A.-J. Arnaud (eds.), *Law, Justice, and Culture*. Stuttgart: Franz Steiner Verlag.

Wacks, Raymond. 2000. Are judges morally accountable? In *Law, Morality and the Private Domain*. Hong Kong: Hong Kong University Press.

Wacks, Raymond. 2009. Injustice in robes: Iniquity and judicial accountability. *Ratio Juris*, 22, 128.

Wacks, Raymond. 2019. *The Spectator*, 28 September, letter to the editor.

Wacks, Raymond. 2021a. *Understanding Jurisprudence: An Introduction to Legal Theory*. 6th edition. Oxford: Oxford University Press.

Wacks, Raymond. 2021b. *The Rule of Law Under Fire?* Oxford: Hart Publishing.

Wagner, Jack. 2017. China's Cybersecurity Law: What You Need to Know. *The Diplomat*. 01 June 2017. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ (Visited 10 December 2020).

Wall, David. 2019. *The Chief Constables of England and Wales: The Socio-legal History of a Criminal Justice Elite*. London: Routledge Revivals, Kindle Edition.

Walter. 1972. *Lore and Science in Ancient Pythagoreanism*. Cambridge, MA: Harvard University Press.

Williams, David. 1967. *Keeping the Peace: The Police and Public Order*. London: Hutchinson.

Willoughby, Westel W. 1918. The Prussian theory of government. *American Journal of International Law*, 12(2), 273.

Wolfers, Arnold. 1952. 'National security' as an Ambiguous symbol. *Political Science Quarterly*, 67(4), 481–502.

Wright. 2020. Tom *One in seven public sector computers still running Windows 7 - CRN FOIs* in CRN online edition https://www.channelweb.co.uk/news/4009090/seven-public-sector-computers-running-windows-crn-fois (Visited 12 December 2020).

Xiao Weibing. 2011. *Freedom of Information Reform in China*. Abingdon: Routledge.

Xiao, Weibing. 2018. *Freedom of Information Reform in China*. Routledge Law in Asia. Abingdon: Taylor and Francis.

Xuezhi, Guo. 2014. *China's Security State*. Cambridge: Cambridge University Press, Reprint.