Chapter 12
Cybersecurity and Cyber Warfare: The Ethical Paradox of 'Universal Diffidence'

George Lucas

Abstract In lieu of the present range of rival and only partial ethical accounts, this essay proposes an underlying interpretive framework for the cyber domain as a Hobbsean state of nature, with its current status of unrestricted conflict constituting a 'war of all against all'. The fundamental ethical dilemma in Hobbes's original account of this "original situation" was how to bring about the morally required transition to a more stable political arrangement, comprising a rule of law under which the interests of the various inhabitants in life, property and security would be more readily guaranteed. Hobbes described opposition to this morally requisite transition as arising from 'universal diffidence', the mutual mistrust between individuals, coupled with the misguided belief of each in his or her own superiority. His is thus a perfect moral framework from which to analyse agents in the cyber domain, where individual arrogance often seems to surpass any aspirations for moral excellence. With this framework in place, it is briefly noted that the chief moral questions pertain to whether we may already discern a gradual voluntary recognition and acceptance of general norms of responsible individual and state behaviour within the cyber domain, arising from experience and consequent enlightened self-interest (As, for example, in the account of emergent norms found in Lucas (The ethics of cyber warfare. Oxford University Press, New York, 2017)), or whether the interests of the responsible majority must eventually compel some sort of transition from the state of nature by forcibly overriding the wishes of presumably irresponsible or malevolent outliers in the interests of the general welfare (the moral paradox of universal diffidence).

Keywords Cyber conflict · Cyber vandalism · Cyber warfare · State-sponsored hacktivism · Stuxnet

G. Lucas (✉)
U.S. Naval Academy & Naval Postgraduate School, Annapolis, MD, USA

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_12

12.1 Introduction

> ….in the nature of man, we find three principall causes of quarrel. First, Competition; Secondly, **Diffidence**; Thirdly, Glory. …Nature hath made men so equall, in the faculties of body and mind; as that though there bee found one man sometimes manifestly stronger in body, or of quicker mind then another; yet when all is reckoned together, the difference between man, and man, is not so considerable, as that one man can thereupon claim to himself any benefit, to which another may not pretend, as well as he. … For such is the nature of men, that howsoever they may acknowledge many others to be more witty, or more eloquent, or more learned; Yet they will hardly believe there be many so wise as themselves:….from this diffidence of one another, there is no way for any man to secure himself… till he see no other power great enough to endanger him…. (Thomas Hobbes (1651/1968, 183–185))

In this essay, I set out a case that our cybersecurity community is its own worst enemy, and that our security dilemmas, including serious moral dilemmas, have arisen mostly because of our flawed assumptions and methodology (modus operandi). These include what Hobbes (1651/1968) termed "universal diffidence"—a devastating flaw shared by many individuals in the "state of nature" (which the cyber domain certainly is)—combined with a smug antipathy towards ethics and moral reasoning as irrelevant or unimportant dimensions of cybersecurity.

The cybersecurity communities of democratic and rights-respecting regimes encompass some of the most intelligent, capable and dedicated public servants one could imagine. However, our community is also rife with jealousy, competitiveness, insularity, arrogance and a profound inability to listen and learn from one another, as well as from the experiences of mistaken past assumptions. I wish to outline the specific impact of all of these tendencies on self-defence, pre-emptive defence, attribution and retaliation in inter-state cyber conflict, alongside vulnerabilities introduced in the Internet of Things (IoT) (arising especially from the inability to foster robust cooperation between the public/governmental and private spheres, and from the absence of any coordinated government or intergovernmental plan to foster such cooperation, leading to increasing reliance on civil society and the private sector to take up the security slack) (Washington Post 2018).

My discussion briefly ranges across vandalism, crime, legitimate political activism, vigilantism and the rise to dominance of state-sponsored hacktivism. I briefly examine cases of vulnerabilities unknowingly and carelessly introduced via the IoT, the reluctance of private entities to disclose potential 'zero-day' defects to government security organisations; financial and 'smart' contractual 'blockchain' arrangements (including bitcoin and Ethereum, and the challenges these pose to state-regulated financial systems); and issues such as privacy, confidentiality and identity theft. The goal is to enable a productive and constructive dialogue among both contributors and readers of this volume on this range of important security and ethics topics. I begin by commenting on the discipline and concerns of ethics itself and its reception within the cybersecurity community, including my earlier treatment of ethics in the context of cyber warfare.

12.2 Ethics and Individuals in the Cyber Domain

At first blush, nothing could seem less promising than attempting to discuss ethics in cyber warfare. Even apart from the moral conundrums of outright warfare, the cyber domain in general is often described as a 'lawless frontier' or a 'state of nature' (in Hobbes's sense), in which everyone seems capable in principle of doing whatever they wish to whomever they please without fear of attribution, retribution or accountability. When it comes to human behaviour and the treatment of one another, human behaviour within the cyber domain might aptly be characterised, as above, as a 'war of all against all'.

Upon further reflection, however, that grim generalisation is no more or less true than Hobbes's own original characterisation of human beings themselves in a state of nature. The vast majority of actors in the cyber domain are relatively benign: they mind their own business, pursue their own ends, do not engage in deliberate mischief, let alone harm, do not wish their fellow citizens ill, and generally seek only to pursue the myriad benefits afforded by the cyber realm: access to information, goods and services, convenient financial transactions and data processing, and control over their array of devices, from cell phones, door locks, refrigerators and toasters to voice assistants such as Alexa and Echo, and even swimming pools.

Beyond this, there are some 'natural virtues' and commonly shared definitions of the Good in the cyber domain: anonymity, freedom and choice, for example, and a notable absence of external constraints, restrictions and regulations. These are things that cyber activists, in particular, like to champion, and seem determined to preserve against any encroachments upon them in the name of the 'rule of law'. In essence, we might characterise the cyber domain as being colonised by libertarians and anarchists who, if they had their way, would continue to dwell in peace and pursue their private and collective interests without interference.

Like all relatively ungoverned frontiers, however, this Rousseauvian bliss is shattered by the malevolent behaviour of even a few 'bad actors'—and there are more than a few of these in the cyber domain. As portrayed in the forthcoming book by Australian cybersecurity experts Seumas Miller and Terry Bossomaier (2019), the principal form of malevolent cyber activity is criminal in nature: theft, extortion, blackmail, vandalism, slander and disinformation (in the form of trolling and cyber bullying), and even prospects for homicide (see also Chap. 11). The widespread chaos and disruption of general welfare wrought by such actors in conventional frontier settings (as in nineteenth century North America and Australia, for example) led to the imposition of various forms of 'law and order'. These ranged from the formation of a posse of ordinary citizens armed with legal authority, engaging in periodic retaliation against criminals, to the election of a Sheriff (or the appointing by government officials of a Marshal) to enforce the law and imprison law-breakers. The eventual outcome of such procedures and interim institutions ultimately led to the more familiar and stable institutions and organisations such as police, courts and prisons to effect punishment, protect the general population from wrong-doers and generally to deter crime.

The control of such malevolent actors and the provision of security against their actions is not primarily a matter of ethics or moral argument (although important moral issues, such as interrogation, torture and capital punishment, do arise in the pursuit of law enforcement). Rather, as Aristotle first observed, for those lacking so much as a tincture of virtue, there is the law. Law, on Aristotle's account, defines the minimum standard of acceptable social behaviour, while ethics deals with aspirations, ideals and excellences that require a lifetime to master. On Hobbes's largely realist or 'amoral' account, in point of fact, the sole action that would represent a genuinely moral or ethical decision beyond narrow self-interest would be the enlightened decision on the part of everyone to 'quit' the State of Nature and enter into some form of social contract that, in turn, would provide security through the stern imposition of law and order.

However law and order, let alone legal institutions such as the police, judges and courts, are precisely what the rank and file individual actors and non-state organisations (such as 'Anonymous') in the cyber domain wish to avoid. This is a very stubborn illustration of widespread 'diffidence' on the part of cyber denizens. I look forward to seeing how Miller and Bossomaier (2019) address this dilemma.

12.3 Ethics and Inter-State Relations in the Cyber Domain

When we turn to international relations (IR), we confront the prospect of cyber warfare. The malevolent actors are primarily rogue nations, terrorists and non-state actors (alongside organised crime). The reigning theory of conflict in IR generally is Rousseau's metaphorical extension of Hobbes from individuals to states: the theory of international anarchy or 'political realism'. There is one significant difference. Although the 'state of nature' for individuals in Hobbes's account is usually understood as a hypothetical thought experiment (rather than an attempt at a genuine historical or evolutionary account), in the case of IR, by contrast, that condition of ceaseless conflict and strife among nations (as Rousseau first observed) is precisely what is actual and ongoing.

Conflict between international entities on this account naturally arises as a result of an inevitable competition and collision of interests among discrete states, with no corresponding permanent institutional arrangements available to resolve the conflict beyond the individual competing nations and their relative power to resist one another's encroachments. In addition, borrowing from Hobbes's account of the amoral state of nature among hypothetical individuals prior to the establishment of a firm rule of law, virtually all political theorists and IR experts assume this condition of conflict among nations to be immune to morality in the customary sense of deliberation and action guided by moral virtues, an overriding sense of duty or obligation, recognition and respect for basic human rights, or efforts to foster the common good.

However we characterise conventional state relationships, the current status of relations and conflicts among nations and individuals within the cyber domain

perfectly fits this model: a lawless frontier, devoid (we might think) of impulses towards virtue or concerns for the wider common good. It is a 'commons' in which the advantage seems to accrue to whomever is willing to do anything they wish to anyone they please whenever they like, without fear of accountability or retribution. This seems, more than conventional domains of political rivalry, to constitute a genuine war of all against all, as we remarked above, and yet this was the arena I chose to tackle (or perhaps more appropriately, the windmill at which I decided to tilt) in *Ethics & Cyber Warfare* (Lucas 2017). As Miller and Bossomaier note in their discussion of that work, I made no pretence of taking on the broader issues of crime, vandalism or general cybersecurity. The book itself was actually completed in September 2015. I predicted then, as Miller and Brossomaier do now, that much would change during the interim from completion to publication. That was certainly true from the fall of 2015 to the fall of 2018. The realm of cyber conflict and cyber warfare appears to most observers to be much different now than portrayed even a scant 2 or 3 years ago.

In the summer of 2015, while wrapping up that project, I noted some curious and quite puzzling trends that ran sharply counter to expectations. Experts and pundits had long predicted the escalation of 'effects-based' cyber warfare and the proliferation of cyber weapons such as the Stuxnet virus. The major fear was the enhanced ability of rogue states and terrorists to destroy dams, disrupt national power grids, and interfere with transportation and commerce in a manner that would, in their devastation, destruction and loss of human life, rival conventional full-scale armed conflict (see also Chap. 18). Those predictions preceded the discovery of Stuxnet, but that discovery (despite apparent U.S. and Israeli involvement in the development of that particular weapon as part of 'Operation Olympic Games') was taken as a harbinger of things to come: a future cyber 'Pearl Harbor' or cyber Armageddon.

However, by and large, this is *not* the direction that international cyber conflict has followed (see also Chap. 13). Instead of individuals and non-state actors becoming progressively like nation-states, I noticed that states were increasingly behaving like individuals and non-state groups in the cyber domain: engaging in identity theft, extortion, disinformation, election tampering and other cyber tactics that turned out to be easier and cheaper to develop and deploy, while proving less easy to attribute or deter (let alone retaliate against). Most notably, such tactics proved themselves capable of achieving nearly as much if not more political 'bang for the buck' than effects-based cyber weapons (which, like Stuxnet itself, were large, complex, expensive, time-consuming and all but beyond the capabilities of most nations).

In an article published in 2015 (Lucas 2015), I labelled these curious disruptive military tactics 'state-sponsored hacktivism' (SSH) and predicted at the time that SSH was rapidly becoming the preferred form of cyber warfare. We should consider it a legitimate new form of warfare, I argued, based upon its political motives and effects. It fit Karl von Clausewitz's definition of warfare as politics pursued by other means. We were thus confronted with not one but *two* legitimate forms of cyber warfare: one waged conventionally by large, resource- and technology-rich nations seeking to emulate kinetic effects-based weaponry; the second pursued by clever,

unscrupulous but somewhat less well-resourced rogue states designed to achieve the overall equivalent political effects of conventional conflict. I did not maintain that this was perfectly valid, pleading only (with no idea what lay around the corner) that we simply consider it, and in so doing accept that we might be mistaken in our prevailing assumptions about the form(s) that cyber conflict waged by the militaries of other nations might eventually take. We might simply be looking in the wrong direction or over the wrong shoulder.

Then the Russians attempted to hack the 2016 U.S. presidential election. The North Koreans downloaded the 'Wannacry' software—stolen from the U.S. National Security Agency—from the 'dark web' and used it to attack civilian infrastructure (banks and hospitals) in European nations who had supported the U.S. boycotts launched against their nuclear weapons programme. Really! How stupid were we victims capable of being? SSH had become the devastating 'weapon of choice' among rogue nations, while we had been guilty of clinging to our blind political and tactical prejudices in the face of overwhelming contradictory evidence. We had been taken in; flat-footed; utterly by surprise.

At the same time, readers and critics had been mystified by my earlier warnings regarding SSH. No one, it seems, knew what I was talking about. My editor at Oxford even refused me permission to use my original subtitle for the book: *Ethics & The Rise of State-Sponsored Hacktivism*. This analysis had instead to be buried in the book chapters. I managed, after a fashion, to get even! When the book was finally published in the immediate aftermath of the American presidential election in January of 2017, I jokingly offered thanks to my (unintentional) "publicity and marketing team": Vladimir Putin, restaurateur Yevgeny Prigozhin, the FSB, PLA Shanghai Unit 61384 (who had stolen my personnel files a few years earlier, along with those of 22 million other U.S. government employees), and the North Korean cyber warriors, who had by then scored some significant triumphs at our expense. State-sponsored hacktivism had indeed, by that time, become the norm.

Where, then, is the ethics discussion in all this? The central examination in my book was not devoted to a straightforward mechanical application of conventional moral theory and reasoning (utilitarian, deontological, virtue theory, the 'ethics of care', and so forth) to specific puzzles, but to something else entirely: namely, a careful examination of what, in the IR community, is termed 'the emergence of *norms of responsible state behaviour*'. This, I argued, was vastly more fundamental than conventional analytic ethics. Such accounts are not principally about deontology, utility and the ethical conundrum of colliding trolley cars. They consist instead of a kind of historical moral inquiry that lies at the heart of moral philosophy itself, from Aristotle, Hobbes, Rousseau and Kant to Rawls, Habermas —and the book's principal intellectual guide, the Aristotelian philosopher, Alasdair MacIntyre.

The great puzzle for philosophers is, of course, *how* norms can be meaningfully said to '*emerge*?' Not just where do they come from or how do they catch on but *how can such a historical process be valid* given the difference between normative and descriptive guidance and discourse? The entire discussion of norms in IR seems to philosophers to constitute a massive exercise in what is known as the 'naturalistic fallacy'. In its original formulation by the Scottish Enlightenment philosopher

David Hume, the fallacy challenges any straightforward attempt to derive duties or obligations straightforwardly from descriptive or explanatory accounts—in Hume's phraseology, one cannot (that is to say) derive an 'ought' straightforwardly from an 'is'.

This is precisely what the longstanding discussion of emergent norms in IR does: it claims to discern action-guiding principles or putative obligations for individual and state behaviour merely from the prior record of experiences of individuals and states. This central conception of IR regarding what states themselves do, or tolerate being done, is thus a massive fallacy. That is to say, states may in fact be found to behave in a variety of discernible ways, or likewise, may in fact be found to tolerate other states behaving in these ways. Certain such behaviours—such as, famously, the longstanding practice of granting immunity from punishment or harm to a foreign nation's ambassadors—may indeed come to be regarded as 'customary'. However, that set of facts alone tells us nothing about what states *ought* to do, or to tolerate. We might claim to be *surprised* if a nation suddenly turns on an adversary state's ambassadors by killing or imprisoning them. However, there are no grounds in the expectations born of past experience alone for also expressing *moral outrage* over this departure from customary state practice. Yet, these kinds of incidents (departure from custom) occur all the time, and the offending state usually stands accused of violating an 'international norm of responsible state behaviour'. Perhaps they have, but there is nothing in the customary practice itself that provides grounds for justifying it as a norm—not, at least on Hume's objection, unless there is something further in the way of evidence or argument to explain how the custom comes to enjoy this *normative* status.

Perhaps my willingness to take on this age-old question and place it at the heart of contemporary discussions of cyber conflict is why so few have bothered to read the book! Who (we might well ask) cares about all that abstract, theoretical stuff? It seems more urgent (or at least, less complicated and more interesting) either to discuss all the latest 'buzz' concerning zero-day software vulnerabilities in the IoT, or else to offer moral analysis of specific cases in terms of utility, duty, virtue and those infamous colliding trolley cars—merely substituting, perhaps, driverless, robotic cars for the trolleys (and then wondering, "should the autonomous vehicle permit the death of its own passenger when manoeuvring to save the lives of five pedestrians", and so forth).

In any event, in order to make sense of this foundational theory of emergent norms in IR, I found it necessary to discuss the foundations of just war theory and the morality of exceptions or exceptionalism (i.e. how do we justify sometimes having to do things we are normally prohibited from doing?), as well as the IR approach to 'emergent norms' itself, as in fact, dating back to Aristotle, and his discussion of the cultivation of moral norms and guiding principles within a community of practice, *characterised by a shared notion of the good* (what we might now call a shared sense of purpose or objectives). Kant, Rawls and Habermas were invoked to explain how, in turn, a community of common practice governed solely by individual self-interest may nevertheless evolve into one characterised by the very kinds of recognition of common moral values that Hobbes had also implicitly invoked to explain

the transition from a "nasty, brutish" state of nature to a well-ordered commonwealth.

I believe that these historical conceptions of moral philosophy are important to recover and clarify, since they ultimately offer an account of *precisely the kind of thing we are trying to discern now within the cyber domain.* That is, the transition (or rather, the prospect for making one) from a present state of reckless, lawless, selfish and ultimately destructive behaviours towards a more stable equilibrium of individual and state behaviour within the cyber domain that contributes to the common good, and to the emergence of a shared sense of purpose. Kant called this evolutionary learning process 'the Cunning of Nature', while the decidedly Aristotelian philosopher Hegel borrowed and tweaked Kant's original conception under the title, 'the Cunning of History'. Their argument is very similar to that of Adam Smith and the 'invisible hand': namely, that a community of individuals merely pursuing their individual private interests may come nevertheless, and entirely without their own knowledge or intention, to engage in behaviours that contribute to the common good, or to a shared sense of purpose.[1]

Finally, in applying a similar historical, experiential methodology to the recent history of cyber conflict from Estonia (2007) to the present, I proceeded to illustrate and summarise a number of norms of responsible cyber behaviour that, indeed, seem to have emerged, and caught on—and others that seem reasonably likely to do so, given a bit more time and experience. Even the turn away from catastrophic destruction by means of kinetic, 'effects-based' cyber warfare (of the catastrophic kind so shrilly predicted by Richard Clarke and others) and instead towards SSH as the preferred mode of carrying out international conflict in cyber space, likewise showed the emergence of these norms of reasonable restraint. Such norms do far less genuine harm, while achieving similar political effects—not because the adversaries are 'nice', but because they are clever (somewhat like Kant's 'race of devils', who famously stand at the threshold of genuine morality).

This last development in the case of cyber war is, for example, the intuitive, unconscious application by these clever 'devils' of a kind of proportionality criterion, something we term in military ethics the 'economy of force', in which a mischievous cyber-attack is to be preferred to a more destructive alternative, when available—again, not because anyone is trying to 'play nice', but because such an attack is more likely to succeed and attain its political aims without provoking a harsh response. However, such attacks, contrary to Estonia (we then proceed to reason) really should be pursued only in support of a legitimate cause, and not directed against non-military targets (I am not happy about the PLA stealing my personnel files, for example, but I am—or was, after all—a federal employee, not a private citizen—and in any case, those files may be more secure in the hands of the PLA than they were in the hands of the U.S. Office of Personnel Management). And thus is the evolutionary emergence of moral norms, Kant's 'cunning of nature' (or

[1] It bears mention that MacIntyre himself explicitly repudiated my account of this process, even when applied to modern communities of shared practices, such as professional societies. I detail his objections and our discussions in the book itself.

Hegel's 'cunning of history') at last underway. Even a race of devils can be brought to simulate the outward conditions and constraints of law and morality—if only they are 'reasonable' devils. (I apologise if I find the untutored intuitions and moral advances of those 'reasonable' and clever devils more morally praiseworthy than the obtuse incompetence of my learned colleagues in both moral philosophy and cybersecurity, who should already know these things!)

12.4 Privacy, Vulnerability and the 'Internet of Things'

Oddly, and despite all the hysteria surrounding the recent Russian interference in the electoral affairs of western democracies, this makes cyber warfare among and between nations, at least, look a lot more hopeful and positive from the moral perspective than the broader 'law and order' problem in the cyber domain generally. Reasonably responsible state actors and agents with discernable, justifiable goals, finally, act with greater restraint (at least from prudence, if not morality), than do genuinely malevolent private, criminal actors and agents (some of whom apparently just want to see the world burn). Here, what might be seen as the moral flaw or failing of 'universal diffidence' is the reckless, thoughtless manner in which we enable such agents and render ourselves vulnerable to them through careless, unnecessary and irresponsible innovations within the IoT.

What I mean is this: technically, almost any mechanical or electrical device can be connected to the Internet: refrigerators, toasters, voice assistants like Alexa and Echo, 'smart' TVs and DVRs, dolls, 'cloud puppets' and other toys, baby monitors, swimming pools, automobiles and closed-circuit cameras in the otherwise-secure corporate board rooms—*but should they be? Do they really need to be?* Moreover, does the convenience or novelty thereby attained justify the enhanced security risks those connections pose, especially as the number of such nodes on the IoT will soon vastly exceed the number of human-operated computers, tablets and cell phones? This appears to be a form of incipient, self-destructive madness.

Miller and Bossomaier, in their forthcoming book on cybersecurity, offer the amusing hypothetical example of GOSSM: the "Garlic and Onion Storage and Slicing Machine". This imaginary device is meant to be stocked with raw onions and garlic, and will deliver chopped versions of such conveniently, on demand, without tears. The device's design engineers seek to enhance its utility and ease of use by connecting it via the Internet to a cell phone app, providing control of quantities in storage in the machine, fineness of chopping, etc. The app connects via the cellphone to the Internet. When the owner is in the supermarket, GOSSM alerts the owner via text message if more garlic or onions should be purchased. The device is simple and handy, and costs under $100 and thus typifies the range of devices continually being added (without much genuine need or justification) to the Internet.

However, in order to provide all that web-based functionality at low cost, the machine's designers (who are not themselves software engineers) choose to enable this Internet connectivity feature via some ready-made open-source software

modules, merely tweaking them to fit. The device is not designed to operate through the owner's password-protected home wireless router. Instead, it links directly to the user's cell phone app, and hence to the Internet, via the cellular data network. Its absence of even the most rudimentary security software, however, makes it, along with a host of other IoT devices in the user's home, subject to being detected online, captured as a zombie and linked in a massive botnet, should some clever, but more unreasonable devil choose to do so.

In October 2016, precisely such a botnet constructed of IoT devices was used to attack Twitter, Facebook and other social media along with large swaths of the Internet itself, using a virus known as Mirai to launch crippling DDoS attacks on key sites, including Oracle's DYN site, the principal source of optimised Domain Name Servers and the source of dynamic Internet protocol addresses for applications such as Netflix and LinkedIn. More recently, in April of 2018, a new Mirai-style virus known as 'Reaper' was detected, compromising IoT devices in order to launch a botnet attack on key sites in the financial sector.[2]

Such events are little more than nuisances, however, when compared with prospects for hacking and attacking driverless cars, or even the current smart technology on automobiles, aircraft and drones. Meanwhile, a new wave of industrial espionage has been enabled through hacking into the video cameras and smart TVs used in corporate boardrooms throughout the world to listen in to highly confidential and secret deliberations ranging from corporate finances to innovative new product development. We have done all this to ourselves, with hardly a thought other than the rush to make exotic functionality available immediately (and leaving the security dimensions to be backfilled afterwards).

Meanwhile, the advent of quantum computing (QC) technology is liable to have an enormous impact on data storage and encryption capacities. Should QC become a reality, the density of storage will increase dramatically, enabling vast amounts of data (even by today's standards) to become available for analysis and 'data mining', while vastly increased process speeds will enable hackers to break the codes of even the most sophisticated encryption software presently available. Encrypted *https://* sites, currently the backbone of Internet commerce, will quickly become outmoded and vulnerable. E-commerce itself, upon which entire commercial sectors of many of the most developed nations depend at present, could grind to a halt.

One likely victim of new security breaches attainable by means of these computational advances would likely be the 'blockchain' financial transactions carried out with cryptocurrencies such as *Bitcoin*, along with the so-called 'smart contracts' enabled by the newest cryptocurrency, *Ethereum*. The latter, for example, is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality, which delivers payments when some third-party, publicly verifiable condition is met.

[2] Zack Whittaker for Zero Day (5 April 2018): https://www.zdnet.com/article/new-mirai-style-botnet-targets-the-financial-sector/ (last access July 7 2019)

This newest cryptocurrency claims to offer total financial transparency and a consequent reduction in the need for individual trust in financial transactions, eliminating (on the one hand) any chance of fraud, censorship or third-party interference. However, as implied above, the opportunities for hacking and disruption of such transactions, creating instability in the currencies and enabling fraud and theft, are likely when increased use of such currencies and transactions are combined with the enhanced power of quantum computing. Preventing that sort of cybercrime, however, would rely on a much more robust partnership between the private and government sectors, which would, in turn, appear to threaten users' privacy and confidentiality. Thus, the prospective solution to the new vulnerabilities would paradoxically impede one of the main present benefits of these cyber alternatives to conventional banking and finance.

Interestingly, we have witnessed Internet firms such as Google, and social media giants such as Facebook and Twitter, accused in Europe of everything from monopolistic financial practices to massive violations of privacy and confidentiality. However, these same private firms, led by Amazon and Google in particular, have taken a much more aggressive stance on security strategy than have many democratic governments in Europe and North America. Meanwhile, for its part, the U.S. government sector, from the FBI to the National Security Agency, has engaged in a virtual war with private firms such as Apple to erode privacy and confidentiality in the name of security by either revealing or building in encryption 'back doors' through which government agencies could investigate prospective wrong-doing. The private firms have been understandably reluctant to reveal their own 'zero-day' vulnerabilities in new software and products, lest doing so undermine public confidence in (and market for) their products.

Their reluctance to do so has only increased in light of a growing complaint that the entire international government sector (led by the U.S. under President Trump) seems to have abandoned the task of formulating a coherent and well-integrated strategy for public and private security. A coherent cyber policy would require, at minimum, a far more robust public-private partnership in cyber space (as noted above), as well as an extension of the kind of international cooperation that was achieved through the 2001 Convention on Cyber Crime (CCC), endorsed by some sixty participating nations in Bucharest in 2001. We need that kind of public-private partnership extended across national boundaries to enable the identification, pursuit and apprehension of malevolent cyber actors, including rogue nations as well as criminals. In the absence of such a collaborative agreement at present, trolls, hackers, vigilantes, and rogue nations are enjoying a virtual field day.

Instead, in an effort to counter these tendencies and provide for greater security and control, European nations have, as mentioned, simply sought to crack down on multinational Internet firms such as Google, while proposing to reassert secure national borders within the cyber domain itself. Generating border controls in this featureless and currently nationless domain is presently possibly only through the empowerment of each nation's CERT (computer emergency response team) to construct Internet gateway firewalls. Such draconian restrictions on cyber traffic across national borders are presently the tools of totalitarian regimes such as China, Iran

and North Korea, which do indeed offer 'security' entirely at the expense of individual freedom and privacy.

All of the concerns sketched above number among the myriad moral and legal challenges that accompany the latest innovations in cyber technology, well beyond those posed by war fighting itself.

12.5 Our Own Worst Enemy

In light of this bewildering array of challenges, it is all too easy to lose sight of the chief aim of 'the Leviathan' (strong central governance) itself in Hobbes's original conception. That goal was not simply to contain conflict but to establish a secure peace. It is perhaps one of the chief defects of the current discussion of cyber conflict that the metaphor of war (as well as the discussion of possible acts of genuine warfare) has come to dominate that discourse (see also Chap. 13). However, our original intention in introducing the 'state of nature' image was to explore the prospects for peace, security and stability—outcomes which hopefully might be attained without surrendering all of the current virtues of cyber practice that activists and proponents champion.

But if peace is ultimately what is desired in the cyber domain, our original Hobbesean problem or paradox remains its chief obstacle: namely, how are we to transition from the state of perpetual anarchy, disruption, and the 'war of all against all' within the cyber domain in a manner that will simultaneously ensure individual privacy, security, and public confidence? In that domain, as we have constantly witnessed, *the basic moral drive to make such a transition from a state of war to a state of peace is almost entirely lacking*. Advocates of greater law and order are metaphorically 'shouted down' by dissidents and anarchists (such as the vigilante group, *Anonymous*) or their integrity called into question and undermined by the behaviour of organisations such as *WikiLeaks*.

For my part, I have not been impressed with the capacities of our most respected experts, in their turn, to listen and learn from one another, let alone to cooperate or collaborate in order to forge the necessary alliances to promote and foster the peace that Hobbes promised through the imposition of law and order. Instead, as in the opening epigram from the *Leviathan* on diffidence, each such expert seems to think himself or herself to be the wisest, and to seem more interested in individual glory through competition with one another for the limelight than in security and the common good.

The case of the discovery of Stuxnet provides a useful illustration of this unfortunate inclination. Who was the first to finally discover the escape of this worm from Nantez Laboratories? Was it cybersecurity expert Ralph Langner (as he claimed in September 2010),[3] VirusBlokADA's Sergey Ulasen 3 months earlier (as most

[3] See Langner's TED Talk in 2011 for his updated account: https://www.ted.com/speakers/ralph_langner (last access July 7 2019).

accounts now acknowledge),[4] Kaspersky Labs (as Eugene Kaspersky still claims),[5] Microsoft programming experts (during a routine examination of their own Programmable Logic Controller [PLC] software)[6] or Symantec security experts (who, to my mind, have issued the most complete and authoritative report on the worm; Fallieri et al. 2011)? All have gone on record as having been the first to spot this 'worm in the wild' in 2010.

Furthermore, what about the phenomenon of state-sponsored hacktivism? It belatedly garnered attention as a strategy and policy following the U.S. election interference, but had been ongoing for some time prior. Cybersecurity experts in Western countries utterly missed this advent, and did not know at first what to make of it when it was discovered, as they continued to hysterically hype the coming 'Cyber Armaggedon'. No planes have fallen from the sky as the result of a cyber-attack, nor have chemical plants exploded or dams burst in the interim—but lives have been ruined, elections turned upside down and the possible history of humanity forever altered. In my own frustration at having tried for the past several years to call attention to this alteration of tactics by nation-state cyber warriors, I might well complain that the cyber equivalent of Rome has been burning while cybersecurity experts have fiddled.[7]

How many times must we fight the wrong war, or be looking over the wrong shoulder, before we learn to cooperate rather than compete with one another for public acclaim? Each of us may think himself or herself the wisest, but wisdom itself seems to lurk in the interstices of the cyber domain: in the shadows, among those who act and those who humbly discern instead. We can and must do better. The fate of the welfare of human kind—certainly a moral imperative worthy of consideration—hangs in the balance.

---

[4] See the account, for example, on the "Security Aggregator" blog: http://securityaggregator.blogspot.com/2012/02/man-who-found-stuxnet-sergey-ulasen-in.html (last access July 7 2019).

[5] See the Kaspersky Labs video presentation detailing their discovery and analysis of the worm, released in 2011: https://video.search.yahoo.com/yhs/search;_ylt=AwrCwogmaORb5lcAScMPxQt.;_ylu=X3oDMTByMjB0aG5zBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNzYw%2D%2D?p=eugene+kaspersky+on+stuxnet+virus&fr=yhs-pty-pty_maps&hspart=pty&hsimp=yhs-pty_maps#id=29&vid=4077c5e7bc9e96b32244dbcbc0c04706&action=view (last access July 7 2019).

[6] See the account offered in the Wikipedia article on Stuxnet: https://en.wikipedia.org/wiki/Stuxnet#Discovery (last access July 7 2019).

[7] In April 2017, only a few weeks after the appearance of my own book on this transformation (n. 1), General Michael Hayden (USAF Retired), former head of the CIA, NSA, and former National Security Adviser, offered an account of the months of consternation within the Executive branch during the period leading up to the U.S. presidential election of November 2016, acknowledging that cybersecurity experts did not at the time no what to make of the Russian attacks, nor even what to call them. I had just finished a 7-year stint in federal security service, teaching and writing on this topic for the members of that community, evidently to no avail. His 2017 annual Haaga Lecture at the University of Pennsylvania Law School's "Center for Ethics and the Rule of Law" (CERL) can be found at: https://www.law.upenn.edu/institutes/cerl/media.php (last access July 7 2019).

References

Fallieri N, Murchu LO, Chien E (2011) W32.Stuxnet Dossier (version 4.1, February 2011). https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Last access 7 July 2019

Hobbes T (1651/1968) Leviathan, Part I, Ch XIII [61] (Penguin Classics edn, Macpherson CB (ed)). Penguin Press, New York

Lucas G (2015) Ethical challenges of disruptive innovation. State sponsored hacktivism and 'soft' war. In: Blowers EM (ed) Evolution of cyber technologies and operations to 2035. Springer International Publishers, Basel, pp 175–184

Lucas G (2017) The ethics of cyber warfare. Oxford University Press, New York

Miller S, Bossomaier T (2019) Ethics & cyber security. Oxford University Press, Oxford

Washington Post (Saturday 25 Aug 2018) A11