

Prospects for Peace in the Cyber Domain

George Lucas, Senior Fellow

Stockdale Center for Ethics & Leadership, U.S. Naval Academy

Abstract: A fundamental ethical dilemma in Hobbes's original, otherwise strictly amoral account of the State of Nature was how to bring about what appears to be a 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 analyze prospects for attaining Peace in the cyber domain. With his framework in place, we quickly note that the chief moral questions pertain to whether one may already discern a gradual voluntary recognition and acceptance of general norms of responsible individual and state behavior within the cyber domain, arising from experience and consequent enlightened self-interest, 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.

I. Crying "Peace! Peace" when there is no Peace in the Cyber Domain

When we are not engrossed by (for example) the latest technologies available through the Internet of Things, it seems that our reflections concerning the cyber realm turn instead to the endless conflicts and prospects for "virtual war" in that domain. But what of the prospects for peace? To what extent is peace, rather than war, a desirable state in this domain? Even more to the point: how willing are the various agents who populate this domain to invest in efforts aimed at achieving the goal of peace, rather than persisting in their present condition of seemingly endless and intractable strife?

At first, nothing could seem less promising than attempting to discuss "peace" in this context. Even apart from the moral conundrums of outright warfare, the cyber domain generally is often described as a "lawless frontier" or a "state of nature," 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 behavior, and the treatment of one another, human behavior within the cyber domain might aptly be characterized, as above, as a "war of all against all."

Upon further reflection, however, that grim generalization of our actual condition is no more or less true than Hobbes's own original characterization of human beings themselves in a hypothetical state of nature. If we stop to consider it, 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 to door locks, refrigerators and toasters, voice assistants like 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 seemed determined to preserve against any encroachments upon them in the name of the “rule of law.” In essence, we might characterize the cyber domain as colonized 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 natural tranquility is easily shattered by the malevolent behavior of even a few bad actors. And there are more than a few “bad actors” in the cyber domain. As a forthcoming book by Australian cyber security experts Seumas Miller and Terry Bossomaier portrays the matter,¹ the principle 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.

Phillip von Wussow accordingly writes in this issue that the “warfare” in question within the cyber domain is that described by Thomas Hobbes, rather than the more recent and conventional account of war by Karl von Clausewitz. For the latter, war is an outgrowth of the natural conflict between clearly-defined competing political policies of well-organized states. For Hobbes, in contrast, the condition of “war” is the natural condition of human agents apart from political institutions, dwelling in anarchy and in the absence of any discernable authority or rule of law.

In contrast to the customary hypothetical invocations by modern political philosophers, however, cyber conflict at present does not constitute some hypothetical “supposing” or fictitious “original position,” affording a privileged vantage point for “reason” to adjudicate matters of fact. Rather, the cyber domain itself now confronts us with the first truly actual and accurate *instance* of such state or condition. A state of nature, accurately characterized by the *bellum omnium contra omnes*, is no more and no less what the cyber realm itself is.

In a fascinating sense, then, the cyber realm, with its many examples of conflict and lack of structure, also unintentionally provides us with the first authentic laboratory in which to examine the chief challenges and puzzle of the *Leviathan* itself: namely, how *does* civil society, social order and the rule of law manage to emerge from such a condition of primordial anarchy? After all, the underlying (if implicit) question in the *Leviathan* is: “what, in this miserable, fallen world of ceaseless conflict, are the prospects for peace?” And if it is peace, security, safety, as guaranteed through the rule of law that is the ultimate goal of the *Leviathan*, how is that goal to be attained?

When we, like Professor von Wussow, invoke Hobbes descriptively, we are likewise obliged to consider the *normative* dimension in his investigations that is quite often forgotten. It is an admittedly thin moral conception for a philosopher famed for his rejection of morality otherwise, but it is a moral conception nonetheless: the obligation incumbent upon all who dwell within this state of nature (as Hobbes editorializes) “to quit it with the utmost dispatch.” Confronted with our natural condition, he argues, we are not permitted to remain in it, but to transform it into something more stable and secure. 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 sort of social contract that, in turn, would provide security through the stern imposition of law and order.

But here we encounter what might be termed the “reality paradox” in the cyber domain. Unlike Hobbes’s fictional individuals languishing unpleasantly in a hypothetical state of nature, “law and order,” let alone legal institutions like police, judges and courts, are precisely what the rank and file individual actors and non-state organizations (like “Anonymous”) in the cyber domain *assiduously wish to avoid*. Hobbes’s own solution to the problem of anarchy is likewise not one that any self-respecting cyber citizen would care to embrace: namely, that a well-regulated civil society will only be achieved through the forceful imposition of authoritarian rule. We have witnessed how nations like China currently attempt the Hobbesian formula in the cyber domain, with limited success. But that approach is not only anathema to democratic and rights-respecting societies – it would represent a fundamental betrayal of what we called earlier the natural virtues and limited natural rights valued by denizens of the cyber domain: liberty, anonymity, privacy, and behavior largely free from interference by others. There are no boundaries, and no governments in cyber space, and cyber citizens profess themselves unwilling to countenance, or yield to such impositions, whatever the Chinese government may attempt.ⁱⁱ

A famous, if persistent problem with Hobbes is that the transition from anarchy to civil society is never really adequately explained. On the one hand, Hobbes appears to argue that the transition will occur pretty much as a matter of course, when inhabitants see their own self-interests optimized by sacrificing some of their freedom and rights in exchange for authoritarian-sponsored state security. But, at the same time, Hobbes recognizes that there is no guarantee that this benign transition will automatically occur. Some, the most malevolent in particular, will be resistant. The truly powerful, the strongest, in the state of nature will never willingly yield their personal authority to the rule of law, simply because it can never be, or be seen to be, in their own individual self-interest to do so.

In contrast to our “reality paradox” in the cyber domain above, this inconsistency generates what is generally known as the “Hobbesian paradox:” i.e., in order to achieve what would clearly be in the self-interests of all, *some act of force* must be utilized to override the narrowly-conceived self-interests of bullies and tyrants in the state of nature. Who, in the state of nature, will consent to dispatch the tyrants and bullies? And how may the rest of us retain confidence that any individual volunteer *willing* to do so, *will* do so without simply assuming their place? The moral imperative – the only moral imperative that Hobbes acknowledges – is that this transition to civil society be made. But apparently it cannot be made. Or at least, there is no clear path, nor ironclad guarantee, that it either can or will take place.

II. Emergent Norms for Cyber Conflict

When we turn to cyber conflict from the perspective of international relations (IR), the malevolent actors are primarily rogue nations, terrorists and non-state actors (alongside organized 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, however, between Hobbes and Rousseau on this condition of international anarchy. 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 international relations, 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 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 basic human rights, or efforts to foster the common good.

However we characterize conventional state relationships, the current status of relations and conflicts among nations and individuals within the cyber domain perfectly also fits this model: a lawless frontier, devoid (we might think) of impulses toward 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.

Beginning in the summer of 2014, while working on my own study of cyber warfare,ⁱⁱⁱ 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 like 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. 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.

But I began to notice that, by and large, this is *not* the direction that international cyber conflict had followed. Instead of individuals and non-state actors becoming more and more like nation-states, I noticed that states were increasingly behaving more and more 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,^{iv} I labeled 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. SSH, for example, perfectly fitted Karl von Clausewitz’s aforementioned 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 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: allowing 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.

And then the Russians attempted to hack the 2016 U.S. presidential election. The North Koreans proceeded to download 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 program. 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. And we had been taken in, flat-footed, utterly by surprise.

At the same time, readers (of which there were not very many) 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 thanked my publisher’s “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!

But where is the ethics discussion in all this? The central examination in my book was not devoted to 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 behavior*.” This, I argued, was vastly more fundamental than conventional analytic ethics. Such accounts are not about principally about deontology, utility, and colliding trolley cars. They consist instead in 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 principle 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? Perhaps my willingness to take on this age-old question and place it at the heart of contemporary discussions of cyber conflict is why few have bothered to read the book! Who cares about all that abstract, theoretical stuff? We either want to discuss all the latest “buzz” concerning zero-day software vulnerabilities in the Internet of Things, or offer our moral analysis 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 maneuvering to save the lives of five pedestrians,” and so forth].

Instead, 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, characterized by a shared notion of the good. 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 characterized by the very kinds of recognition of common moral values that Hobbes, as well, had implicitly invoked to explain the transition from a “nasty, brutish” state of nature to a well-ordered commonwealth – *precisely the kind of thing we are trying to discern now within the cyber domain*. 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.”

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 summarize a number of norms of responsible cyber behavior 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 (as shrilly predicted by Richard Clarke and others) and toward SSH instead as the preferred mode of international conflict, likewise showed the emergence of these norms of reasonable restraint – doing far less genuine harm, while achieving similar political effects – not because we are “nice,” but because we are clever, 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. But 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’m not happy about the PLA stealing my personnel files, but I am – or was, after all – a federal employee, not a private citizen). And the evolutionary emergence of moral

norms, Kant's "cunning of nature," (or Hegel's "cunning of history") is thus 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.

III. Conclusion: the Hobbesian Paradox

Once again, critics may view this account of emergent norms as being nearly as thin a conception of morality as that of Hobbes's attempt to encourage rogues and villains to embrace the rule of law. I cannot quarrel with this finding: morality is clearly treading on thin ice within the cold reaches of cyber space. But what is the alternative?

We would need to countenance an act of monumentally immoral proportions in response to the moral outrage most of us might feel at being held perpetual hostages in cyber space: our property, security, even our personal identities – as well as our public institutions and civil discourse and political decision-making – incorrigibly at risk to hijacking, theft, and corruption by unscrupulous persons, organizations, and rogue nations. This seems unacceptable, and so some act of intervention, forceful intervention, must be contemplated and ultimately attempted. But by whom, and upon what authority? Are all nations compelled to reassert national borders, and build virtual "firewalls" around them to keep out intruders (and to keep their own citizens and inhabitants in line)? This seems also unacceptable.

Either we acknowledge and nurture the fragile norms that grow up in the thin moral soil of cyber space, or else we colonize and tyrannize this new domain, forcing legal compliance at the expense of its most promising virtues.

ⁱ *Ethics & Cyber Security* (Oxford: Oxford University Press, forthcoming 2019).

ⁱⁱ It bears mention that China, for its part, has accused the U.S. and western allies of attempting to impose its own form of hegemony on the "commons" that is the cyber domain, in exercises like the Tallinn Manual on International Law applicable to that domain. The official view is that cyber space is a "commons" in which all actors (individuals, collectivities, and nations) may act without restriction. That international view, however, is inconsistent with their domestic practice.

ⁱⁱⁱ Since published: *Ethics & Cyber Warfare* (Oxford: Oxford University Press, 2017).

^{iv} "G.R. Lucas, "Ethical Challenges of 'Disruptive Innovation': State Sponsored Hacktivism and 'Soft' War." *Evolution of Cyber Technologies and Operations to 2035*. Ed Misty Blowers (Basel, SW: Springer International Publishers, 2015). "Advances in Information Security, Vol. 63." Pp. 175-184.