PACEM 20:1 (2017), s. 65-70
ISSN 1500-2322
© Feltprestkorpset

State-Sponsored Hacktivism and «Soft War»

A Moral and Legal Challenge in the Cyber Domain

AV GEORGE LUCAS

Skeptics (e.g., Thomas Rid, 2013) have cast doubt on the notion of authentic cyber *warfare*. Cyber conflict consists, the skeptics argue, solely of activities which fall well short of full scale warfare: e.g., crime, vandalism, «hacktivism» (political activism by individuals and organizations carried out in the cyber domain), industrial espionage, and military espionage. Talk of cyber «warfare,» they complain, is largely conceptual confusion, coupled with misplaced metaphorical exaggeration.

Against such criticisms, I have argued by contrast that there *is* a distinctive category of cyber conflict that qualifies as warfare – or, more correctly, which rises to the level of the «use, or threat of use, of force by states; or, the equivalent of an armed attack» in international law (Lucas 2017). This new kind of warfare has thus far manifest itself in two distinctive forms:

1. *effects-based* weapons (such as Stuxnet) which can be deployed to damage or destroy military targets; and
2. weapons and attacks in the cyber domain intended to produce *political effects* similar to those usually sought as the goal or objective of a conventional use of force by states against one another.

I have labeled this second class of cyber hostilities «*state-sponsored hacktivism»* (SSH). SSH is one of the principle tactics of a wider phenomenon, recently dubbed «soft war,» or unarmed conflict (Gross & Meisels, 2017).[1] It

[1] Policy experts in the U.S. Department of Defense include a variety of soft war tactics, including the various instances of SSH I discuss here, within a general category of conflict they term «grey war»: http://www.defenseone.com/ideas/2015/12/fighting-while-friending-grey-war-advantage-isis-russia-and-china/124787/. This is not a very precise or useful classification, in my view, because it lumps too many disparate tactics under a single umbrella, and thus also fails to distinguish among other important but distinctive types of «soft war.» The latter is the better general descriptor for all of these approaches to unarmed conflict, while SSH is a unique and important element that demands separate attention, for reasons I specify in this article.

qualifies as warfare because it is deployed to compel an adversary to yield to the political aims of the state utilizing it. SSH is perfectly capable of achieving the equivalent of occupying an enemy's cities, destroying his army, and breaking his will to fight. It is fully capable of moving a political center of gravity from a given posture prior to the attack, to one more in keeping with the attacker's own political aspirations *vis á vis* the victim's in the aftermath. In short, this form of cyber conflict satisfies the classical definition of Clausewitz (1830) regarding war as politics carried out by alternative means.

SSH is not identical to, nor can it be merely reduced to acts of vandalism, crime, or espionage, although it utilizes such components within the framework of an SSH attack. One might say that SSH is either *none of the above*, or else it involves *all* of the above «on steroids.» Considerations of scale and magnitude, as well as of ease of access, are important in understanding this category of warfare, much as such considerations have been, in the past, for differentiating between «private» and domestic uses of conventional lethal force (e.g., as criminal acts by individuals or organizations), and those of «public» warfare that are state-sponsored.

The Rise of State-Sponsored Hacktivism

With the benefit of hindsight, we can identify what was likely the first clear instance of SSH in the DDoS attacks, allegedly by agents of the Russian Federation, carried out against Estonia in 2007. The most recent examples include the North Korean attacks upon Sony Pictures and (using similar cyber techniques) on the SWIFT banking system in Europe; the Russian interference in the U.S. and French elections; and the Iranian attacks on ARAMCO and (under the guise of the anonymous «Cyber Fighters of Izz ad-Din al-Qassam») on the U.S. banking system in 2012. Yet another dramatic example of SSH was the theft of some 22 million civilian and military personnel files from the U.S. Office of Personnel management by PLA Unit 78020 in Kunming, China in 2015.

It is extremely important, as Jessica Wolfendale demonstrates, to recognize this and other tactics of «soft war» as authentic warfare, so that one may determine just exactly how to understand and respond to such events (Wolfendale 2017). In this instance, one might think it possible to subsume SSH in particular, and other elements of soft war, under the relatively new category of conventional uses of force that fall short of full-scale war, termed *jus ad vim (*Frowe 2015). But Valerie Morkevičius has shown decisively that soft-war tactics like SSH cannot be so understood or subsumed, because they involve no

use whatsoever of conventional force (Morkevičius 2017). In particular, unlike effects-based cyber weapons and attacks, SSH attacks *do not cause physical harm*. Instead, they disrupt normal social functions, cast doubt and sow fear among the general population, and spread confusion, undermine morale, and otherwise interfere with the normal conduct of government and military personnel and operations.

Ever since the alarm was raised by cyber experts like John Arquilla (1993) and Richard Clarke (2010), we have been anticipating the onslaught of effects-based cyber attacks: a so-called «Cyber Armageddon,» or «cyber Pearl Harbor.» While poised to defend and counter such attacks in our cyber strategy, we have been largely silent on how to understand and respond to SSH. Former CIA and NSA director, General Michael Hayden (U.S. Air Force, retired), delivering the annual Distinguished Haaga Lecture («Russian Meddling in the U.S. Election») at the University of Pennsylvania Law school on 18 April 2017 (https://www.youtube.com/watch?v=Kt36R6DR7Hc), described the U.S. posture toward these alternative attacks as confused and disorganized, admitting that we do not yet know even what to call these types of cyber attacks, let alone has the U.S. developed any kind of coherent strategy to defend or retaliate against them.

Cyber Warfare and Cultural Bias

Some of this difficulty stems from an underlying organizational and cultural bias that blinds us to the significance of SSH. Consider that Israel, the U.S., and its allies in the «Five Eyes» signal intelligence alliance are, collectively, supreme masters of the first kind of cyber warfare. Effects-based weapons like Stuxnet, tactical operations like «Olympic Games», and the recent repeated «mysterious failures» of North Korean intercontinental missile test launches, are all complex, sophisticated, and resource-intensive operations. Very few nations possess the combination of technical expertise and national resources (and perhaps patience) to develop and deploy such weapons. Feeble attempts in this realm by less well-resourced states (an alleged Iranian attack on a small dam in upstate New York in 2013, for example: http://time.com/4270728/iran-cyber-attack-dam-fbi/) did not prove effective.

Large-scale, effects-based weapons are, in short, «our» kind of weapon: big, bold, expensive, intricate and technologically sophisticated, and fully equivalent to conventional war and weapons. By contrast, the weapons and tactics of SSH are comparatively small-scale. These rely more on cleverness, stealth, and

deception bordering on perfidy. They are affordable, accessible, and attainable, and (in comparison to effects-based weapons) easily within reach of adversaries who lack the essential resources, or do not choose to invest those resources, let alone the time and energy necessary to develop high-quality effects-based cyber weapons.

And indeed: why should they bother? SSH attacks have demonstrated that they can accomplish nearly as much «political bang,» for only a fraction of the investment «buck.» Perhaps most significantly, these SSH operations take place just below the threshold of full attribution and retaliation. General Hayden described the months of confusion and uncertainty within the Obama administration over how and when to acknowledge and respond, as the Russian assaults on the presidential election of 2016 were detected and ongoing in the weeks and months leading up to the November 2016 election itself. Officials wondered, «What exactly are they up to, and what should we do about it?» While we ponder these questions in confusion, our adversaries are literally «eating our lunch!»

No effective defense or counter-attack can be readily instituted against a kind of warfare about which we are largely ignorant, and for which we are, at present, wholly unprepared. While we have worried about and waited for the coming «cyber Armageddon,» our adversaries have figuratively «snuck up behind us» and have cleverly instead created disarray in our cyber defenses, ironically by utilizing tactics once thought to be the domain of alienated teenagers and vigilante groups. *And they have done so effectively.* We are presently engaged in what has proven to be a years-long war in the cyber domain in which we (i.e., the U.S., NATO, the E.U., and our allies) have been and are being *roundly defeated at every turn*.

The Failure of International Law

Unlike the advent of effects-based cyber weapons, international law has no clear jurisdiction over SSH. The first *Tallinn Manual* (2013) devoted to examining the application of international humanitarian law (the law of armed conflict) to operations in the cyber domain, clearly identified cyber weapons like Stuxnet as «weapons» in the conventional sense of the term, even though composed of software instead of explosives (Jenkins 2012). It was largely silent on what we are calling SSH, other than commenting that what turns out to be the first incident, the 2007 attack on Estonia, did not rise to the level of a use of force, or an armed attack.

Just as the broader public discussion conflated key elements of cyber conflict, so legal and policy experts now routinely conflate and confuse two very different modes of legitimate warfare in the cyber domain. Lacking this key category of analysis, for example, the successor project, *Tallinn 2.0* (2017), failed to encompass SSH under any of the remaining regimes and resources of international law that it otherwise attempted to bring to bear on cyber conflict generally. Even had SSH been properly identified and differentiated in this otherwise impressive effort, it is not at all clear that present international law would offer much in the way of guidance, governance, or restraint. But no guidance of any sort is possible if we fundamentally misunderstand, and fail to identify and distinguish the sort of behavior we are trying to govern and control.

Ethics and Moral Norms

In *Ethics and Cyber Warfare* (Oxford UP, 2017), I document the rise of SSH, and also attempt to trace the gradual evolution of norms of responsible state behavior in this new and novel context. The (alleged) attack on Estonia in 2007, for example, was utterly indiscriminate and wholly disproportionate to the degree of harm inflicted by the victim state on the aggressor (which itself – the Estonian government's decision to relocate a Russian war memorial – could hardly be said to constitute a *causus belli*). This attack could have been extremely destructive and harmful, although fortunately it ceased before it became so. But had it persisted even a few more hours, let alone spread to other vulnerable cyber sectors of Estonian civil society, it could have resulted in grave injury, massive suffering, immiseration, and even loss of life. Despite some of the more amusing features of the North Korean attack on Sony Pictures, the political implications of that action were potentially serious, and the highly similar cyber techniques subsequent employed to disrupt the SWIFT banking system in Europe (resulting in the theft of $81 billion from an impoverished country which had done nothing whatsoever to bring on such an attack) were extremely grave.

SSH is no laughing matter. It has become the military tactic of choice for an increasingly wide array of unprincipled nation-states, and they, in turn, are becoming ever more proficient masters of this novel warfare tactic. We need to take this threat seriously, and move quickly to avail the international community of the appropriate moral and legal norms with which to understand and restrain this new form of warfare. These, as I argue, have already been embodied in some of the previous and subsequent forms of attack: e.g., an increased willingness to distinguish between military and dual-use targets on one hand,

and wholly civilian objects and institutions on the other, as well as to refrain from engaging in such cyber attacks without legitimate provocation.

These are fragile and tenuous achievements, however, which need to be acknowledged, ratified, endorsed, and strengthened by all parties to cyber conflict. That, to say the least, is a tall order within a domain of otherwise unrestricted conflict, within which warring adversaries claim their right to do whatever they please, to whomever they wish, whenever they want, with little fear of accountability or retaliation. Nevertheless it remains the case, as with conventional warfare, that the recognition and modest restraint of war is the first step toward a just and lasting peace.

References

Arquilla 1993 - John Arquilla and David Ronfeldt: «Cyberwar is coming!», *Comparative Strategy* 12 (no. 2): 141–65.

Arquilla 2012 - John Arquilla: «Cyber War is Already Upon Us,» *Foreign Policy*: (March-April): http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us.

Clarke 2010 - Richard A. Clarke and Robert K. Kanke: *Cyber war: the next threat to national security and what to do about it*. New York: HarperCollins.

Clausewitz 1830 - *On War*. Translated and edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Frowe 2015 - Helen Frowe: *The Ethics of War and Peace: An Introduction*. Oxford: Routledge, 2nd edition.

Gross and Meisels 2017 - *Soft War: the Ethics of Unarmed Conflict*, eds. Michael L. Gross and Tamir Meisels. Cambridge: Cambridge University Press.

Jenkins 2012 - Ryan Jenkins: «Is Stuxnet Physical? Does it Matter?», *Journal of Military Ethics* 12 (1): 68-79.

Lucas 2017 - George Lucas: *Ethics and Cyber Warfare: the Quest for Responsible Security in an Age of Digital Warfare.* New York: Oxford University Press.

Morkevičius 2017 - Valerie Morkevičius: «Coercion, manipulation and harm: civilian immunity and soft war» in *Soft War: the Ethics of Unarmed Conflict*, eds. Michael L. Gross and Tamir Meisels, Cambridge: Cambridge University Press: ch. 2.

Rid 2013 - Thomas Rid: *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Tallinn Manual 2013 - *The Tallinn Manual on the International Law Applicable to Cyber Operations.* Ed. Michael N. Schmitt. New York: Cambridge University Press.

Tallinn 2.0 2017 - *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Ed. Michael N. Schmitt. New York: Cambridge University Press.

Wolfendale 2017 - Jessica Wolfendale, «Defining Soft War,» in *Soft War: the Ethics of Unarmed Conflict*, eds. Michael L. Gross and Tamir Meisels. Cambridge: Cambridge University Press: ch. 1.

George Lucas is Stockdale Professor of Ethics at the U.S. Naval War College (Newport RI USA).