

# JOURNAL OF LAW & CYBER WARFARE

## ARTICLES

Mitigating Moral Hazard in Cyber-Risk Insurance

By Liam M.D. Bailey

The Deregulation and Swarming of Cyberwarfare:

The Need for and Limitations of Law in Enabling Aggressive  
'Hacking-back' and Pre-Emption

By Dr. Mils Hills

Legal Considerations on Cyber-Weapons and Their Definition

By Stefano Mele

Internet Communication Blackout: Attack Under Non-International  
Armed Conflict?

By Cassandra Mix

Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA)  
Inadequacies in Regulating and Enforcing Money Laundering Laws over  
Virtual Currencies and the Internet

By Sheng Zhou

Volume 3 | Spring 2014 | Issue 1

(c) 2013 – 2014. Journal of Law & Cyber Warfare.

All Rights Reserved.

[www.jlcw.org](http://www.jlcw.org)

# EDITORIAL BOARD

## EXECUTIVE EDITORS

*Editor-in-Chief*

Daniel B. Garrie, Esq,

*Executive Editor*

Siddartha Rao, Esq.

*Research Editor*

Radhika Tiwari

## INDUSTRY ADVISORS

|                     |                     |
|---------------------|---------------------|
| Alan Roper          | Jonathan Turner     |
| Cedric Leighton     | Joseph V. DeMarco   |
| Christopher Burgess | Joseph Weiss        |
| Dick Crowell        | Larry Ponemon       |
| Eric Jensen         | Michael Schmitt     |
| Gus Dimitrelos      | Noah Bledstein      |
| Jack Dever          | Richard Borden      |
| James Christiansen  | Russell Walker      |
| Jeff Bardin         | Uma Chandrashekhkar |
| Jeremy Kroll        | Vincent Scott       |
| John Dever          | William Spernow     |

## MEMBERS

Kim Kopoff  
Candice Lang  
Sarah E. Haines  
Stephen Williams  
Valerie Strumwasser  
Margaret Mak  
Salvatore Scibetta

# **The Deregulation and Swarming of Cyberwarfare: The Need for and Limitations of Law in Enabling Aggressive ‘Hacking-back’ and Pre-Emption**

By Dr. Mils Hills<sup>1</sup>

## **Abstract:**

*This conceptual paper seeks to add some critical tone and shades of light and darkness to the considerations associated with ‘hacking-back’ by liberal democratic states. As with counter-insurgency and related operations, the challenges are that whilst state and non-state adversaries may not play by our rules, we will stick to ours. What space does that leave, then, in an era of unrestricted warfare, for aggressive cyber counter-strike and pre-emptive activities? In summary, the need for creativity and innovation should allow the development of tools, tactics and strategy that deliver strategic competitive advantage, cognizant of legal and other controls, constrains and frameworks. As part of a developing pipeline of research conducted at Northampton Business School, UK, the author draws on consultancy and support to elite military units in the UK, those who develop doctrine, concepts and force for the British Army and relevant security organizations in the UK and beyond.*

---

<sup>1</sup> Associate Professor of Risk, Resilience and Corporate Security, Value-Chain Research Group (VCRG), Northampton Business School, University of Northampton, UK [mils.hills@northampton.ac.uk](mailto:mils.hills@northampton.ac.uk).

## I. INTRODUCTION

This paper sets out the context in which liberal democratic states need to be able to draw on an inarguable legal mandate to both respond and pre-empt electronic attacks or attacks on their electronic infrastructure.<sup>2</sup>

In an era of unrestricted warfare, where tools and skills are ever more widely available; where states have lost the monopoly on the use of lethal violence on literal battlefields, and can no longer realistically be said to have the exclusive license to use electronic lethal violence; where our businesses, media, health and other infrastructures may be the (un)intended targets of cyberwarfare; and, perhaps most troublingly, where attacks may well be mounted by those who swarm from a global constituency to actively contribute to a cause, we are faced with a great lack of guidance as to what constitutes an appropriate and legally defensible response. The context is of an acute challenge posed by the ease of swarm activation - *intentionally* mounted by hostile states, activist groups or movements or *unintentionally* when individuals or groups feel the need to add their support to a cause which energizes them.

How can international and domestic, military and civil law prepare for the challenge of ‘hacking back’<sup>3</sup> in this swamp of swarmed activists,<sup>4</sup> hostile states and others

---

<sup>2</sup> This paper is written from the perspective of a non-legal scholar, dimly aware of some of the provisions of the Laws of Armed Conflict (LOAC).

<sup>3</sup> See generally KENNETH E. HIMMA, INTERNET SECURITY: HACKING, COUNTERHACKING, AND SOCIETY 99 (2007) (surveying recent ethical policy issues having to do with the Internet and cybersecurity).

<sup>4</sup> See JOHN ARQUILLA & DAVID RONFELDT, SWARMING AND THE FUTURE OF CONFLICT (2000) available at <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA384989>. (discussing the meaning of swarming (“seemingly

joining the melee? When anyone with a grudge, cause or preoccupation can throw their hat into the ring, take up electronic arms and cleave to the fray, states must anticipate difficult and challenging times ahead. Given the challenge posed by such a swarm, pre-emptive activity by states to disrupt any calls to action, distribute toolkits, and teach skills, etc., could be a beneficial means of risk reduction when a swarm-activation event arises.

Grounded in an appreciation of the need for liberal democratic states to sustain National Strategic Competitive Advantage<sup>5</sup> – as well as enabling the competitive advantage of businesses hosted in our liberal democratic states (who also operate in other jurisdictions) – this paper aims to contribute to law- and policy-makers' thinking in this challenging area. A key conclusion is that law is going to offer little in terms of a panacea to the volume, vectors and velocity of cyberwarfare attacks – a context where attribution may not meet conventional evidential standards and the necessity for counter-strike may be a matter of existential survival rather than ideological or political choice.

---

amorphous, but deliberately structured, coordinated, strategic way to perform military strikes from all directions”) and how a new military doctrine is emerging to take advantage of modern technology and connectivity).

<sup>5</sup> See generally Lawrence E. Casper, et al., *Knowledge-Based Warfare: A Security Strategy for the Next Century*, JOINT FORCES QUARTERLY 81-89 (1996), available at <http://www.au.af.mil/au/awc/awcgate/jfq/1813.pdf> (explaining the dilemma faced by armed forces in maintaining short-term effectiveness while simultaneously preparing for a long-term future in an era of changed and/or declining resources paired with advanced and changing technology).

## II. THE CHALLENGE FOR LIBERAL DEMOCRATIC STATES, THEIR MILITARIES, AND THEIR SECURITY SERVICES

Cyberwarfare was surely never meant to be like this. The barriers to entry are often so low (specifically: time to self-educate is the primary necessity, rewarding the time-rich and cash-poor) and the likelihood of capture and/or punitive measures remains so slight that that almost anyone can and does become involved, whether as hacker, malware designer or (one anticipates) even the targeter of electronic networks via physical destruction or degradation.<sup>6</sup> Warfare and the employment of lethal violence was – once and for a while – the preserve of state-sanctioned militaries. Cyberwarfare – along with compressing time and space – has collapsed distinctions between adversaries and frontlines.<sup>7</sup> As this paper goes to press, Syria has become the latest failing state context to form a more-or-less open playground for a global community of mobile individuals to travel to and undertake whatever forms of violence they care to pursue.

Although reprehensible and revolting as this certainly is, the same phenomenon of self-recruitment to, and action in pursuit of, an adopted cause is seen in the cyber-domain. The electronic front line is everywhere and nowhere all at once. One can become energized to an

---

<sup>6</sup> See generally Tim Jordan & Paul Taylor, *A Sociology of Hackers*, 46, 4 SOCIOLOGICAL REV., 757 (Nov. 1998) (outlining the concept of a hacker community, and the existence of ‘information societies’).

<sup>7</sup> See RAYMOND C. PARKS & DAVID P. DUGGAN, PRINCIPLES OF CYBERWARFARE (2001) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.1478&rep=rep1&type=pdf> (proposing and defining several principles of cyberwarfare, and differentiating it from ‘kinetic warfare’).

agenda and choose to do something about it at any time.<sup>8</sup> I have written elsewhere about how we might explore and challenge the dynamics of such self-recruitment.<sup>9</sup> However, this is not a situation that is likely to change. Indeed, one might argue that it is likely to become considerably more challenging.

For example, just as the collapsed state of Syria now faces the unofficial ‘free for all’ in which anyone is able to enter, join a militia, receive some basic weapons or explosives training and become part of the fray, those charged with countering cyber-warfare and attending to the legal frameworks under which any pre-emption or response would be constructed face equally acute problems. Some states are reacting to the problem of their citizens fighting in the Syrian conflict by threatening to withdraw citizenship.

Can the same principle – buttressed by labelling the activity as terrorism – apply to those who undertake e-terrorism, either deliberately under the flag of a foreign regime, recruited by such a regime, crowd-sourced by outrage at some cause or another, or from some other motivation?<sup>10</sup> What needs to be done about those of our

---

<sup>8</sup> See Dorothy Denning, *Cyberwarriors: Activists and Terrorists Turn to Cyberspace*, XXIII, 2 HARVARD INT’L REV., 70, 70-75 (2001) (using the Palestinian-Israeli conflict of late 2000, which involved hacking attacks, to illustrate the growing use of cyberspace as a digital battleground).

<sup>9</sup> Cf. Mils Hills (2012) *New Perspective on the Achievement of Psychological Effects from Cyber-Warfare Payloads: The Analogy of Parasitic Manipulation of Host Behaviour*, 1, 1 J. OF L. & CYBERWARFARE, 208, 208-217 (2012).

<sup>10</sup> See Mark Manion & Abby Goodrum, *Terrorism or civil disobedience: toward a hacktivist ethic*, 30, 2 ACM SIGCAS COMPUTERS & SOC’Y, 14, 14-19 (Jun. 2000) (investigating the potential of ‘hacktivism’ as a tool in civil disobedience and fights against political injustice).

citizens who feel the need to contribute to their military's or intelligence services' real or imagined actions against an adversary state / organization by joining in an unofficial or vigilante capacity?

The unintended consequences of their actions may be horribly unhelpful and counter-productive or, potentially, may be beneficial. In either case, they would fall outside of protective legal frameworks and yet contribute to escalation potentially directed at different targets once attribution is achieved (or is assumed to have been achieved) by the original target.

### III. ELECTRONIC SELF-DEFENSE

Whilst it appears self-evident that those of our citizens who may feel inspired to become part of a cyber-attack on assumed or known state adversaries will be outside of the employ of the state, it is extremely well-known that in other states, no such distinctions are held. Indeed, the blurring of the private and state-sector in terms of capability may be very significant. If it is assumed that capability is being made ready, trialed or even executed from non-military, non-state locations in adversary states – at what point is it legal to mount aggressive reconnaissance on those locations, pre-position electronic munitions to form a counter-strike, attempt to recruit or gain intelligence on the individuals who work there, and so on? At what point is pre-emptive, self-defensive attack legally legitimate?<sup>11</sup>

---

<sup>11</sup> See David Barnard-Wills & Debi Ashenden, *Securing Virtual Space: Cyber War, Cyber Terror, and Risk*, 15, 2 SPACE & CULTURE 110, 110-123 (May 2012) (arguing that cyberspace may be essentially ungovernable); Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace*, 84, 3 CHICAGO-KENT L. REV. (2010), available at <http://ssrn.com/abstract=1363932> (creating a

How is any legal position on these matters complicated or compromised by the dispersion of, for example, a somewhat or sometimes hostile state-owned, controlled or sympathetic business overseas – in the sovereign jurisdictions of our allies or even in our own state? What damage might we (accidentally) face inflicting on ourselves by targeting businesses that operate at the behest of a foreign power but that *at the same time* provide us or our allies with critical national infrastructure? Are we and our allies conscious of this dependence – even if it is of a second- or third-order? If we target business ‘x’ in a southeast Asian state, might a response come back through business ‘y’, which is not electronically connected with the original target but – being controlled by the host state – is utilized to apply a counter-measure (e.g. withdrawal of a critical national infrastructure service, explained as due to *force majeure* – thus nullifying any contractual leverage)?

Where does the law stand on all of these issues? Indeed, does the legal categorization even matter?

#### IV. THE SIGNAL POWER OF LAW AND ITS LIMITATIONS

Signaling has *something* to offer in terms of broadcasting clear consequences from a sound legal basis to all potential adversaries – and especially those deliberately identifying or considering identifying vulnerabilities in clearly non-military, non-state-owned infrastructure. Adversaries should have much to fear from either aggressive reconnaissance for targeting; probing for vulnerabilities; the brigading of focused capability; or the pre-placement of cyber-munitions or human assets. These and other activities need to be deterred. It may be that

---

model of how the law could allow for hackback, and how parameters might be set for legally permissible retaliatory or defensive hackbacks).

existing domestic laws and, for example, the Laws of Armed Conflict (LOAC) currently provide adequate legal cover or could be adjusted to do so. However, even if this is the case, the situation may not be clearly “signaled.” Even if it were to be so signaled, the challenges of e-attribution and the self-organizing swarm are massive. The deterrence value (in the form of punitive sanctions) of law is of no significance when cyber-warfare is so difficult to attribute and where irritating swarms may self-assemble who, even when employing low-tech scripting and hacking, may cause problems by sheer volume of effort.

An issue to be raised is, then, what form of legally-enabled signaling could dissuade swarming cyber-threats who organize themselves into campaigning structures and potentially have the guiding hand of a hostile power behind them?<sup>12</sup> In the era of unrestricted, unrestrained cyber-warfare (where activists, mercenaries, proxies, criminals, the misguided and others throw their hats into the ring) – what are the cyber-penalties? Is a member of an assembled swarm that causes loss of critical services (e.g. an infrastructure attack resulting in power failure that leads to patients dying in hospitals) culpable for a charge of homicide? Given the low likelihood of most of these culprits being physically apprehended – *how* (given limited investigative resources) can adequate attribution be achieved and *what* would comprise a cyber- or e-sanction, or an e-penalty? What would be the graduated scale? How can semi-permanent e-sanctions or e-penalties be enforced?

Given the backdrop of the hysterical and usually unbalanced criticism of and lack of trust in national technical authorities and others that has arisen as a result of

---

<sup>12</sup> See JAMES A. LEWIS, *ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR AND OTHER CYBER THREATS* (2002), *available at* [http://csis.org/files/media/csis/pubs/021101\\_risks\\_of\\_cyberterror.pdf](http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf) (a reassessment of the threat of cyber war and its potential targets).

Snowden's 'disclosures' – what will domestic, allied and international opinion on the pursuit of the ideas detailed above be? What freedom of maneuver remains? What forces or events could constrain or expand this maneuver space?

## V. CONCLUSION

This thinkpiece paper has sought to problematize any lingering assumptions that legal remedies can flex and stretch to accommodate the threat environment in which our security and military apparatuses operate. However, there may well be some little deterrent value in signaling to would-be adversaries that – thanks to appropriate legal groundings – clear and punitive consequences will flow from any pre-emptive aggressive reconnaissance, let alone actual cyber-warfare attacks. More pragmatically, and somewhat beyond the scope of this paper, crisper signals may well be delivered by having the legally-provided ability to demonstrate to an adversary / mercenary / proxy that one already has the means to deliver punitive sanctions in acutely sensitive areas of their systems.

Given the deregulation of violence (cyber- and otherwise), the reduced barriers to entry for some cyberwarfare activities, and the ease with which swarms can be generated or may form spontaneously, legal deterrence or redress may only have any effect on those regimes who can be encouraged to comply with good behavior through diplomatic and other nonmilitary channels.