Spring February 4, 2015

A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs

Jan Kallberg, *University of Texas at Dallas*

Kallberg, Jan, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," IT Professional , vol.17, no.1, pp.30,35, Jan.-Feb. 2015
doi: 10.1109/MITP.2015.1

A Right to Cyber Counter Strikes

The Risks of Legalizing Hack Back

Jan Kallberg
Cyber Security Research and Education Institute
Erik Jonsson School of Engineering and Computer Science
The University of Texas at Dallas
Richardson, TX 75083-0688
jkallberg@utdallas.edu

The idea to legalize hacking back has gained traction the last years and received several influential corporate and political proponents in the United States and Europe. The growing frustration with repeated cyberattacks and lack of credible law enforcement pushes for alternative ways to prevent future cyberattacks. As of today, counter cyberattacks are illegal in a majority of the nations because it constitutes another cybercrime independent from the initial attack. If cyber counter attacks were legalized it raises a set of questions. The first line of questions are linked to the underlying assumptions that the proposal to legalize counter cyberattacks are based upon. The second line of questions are the embedded challenges to the role of the nation state. Privatized and allowed counter cyberattacks could jeopardize the authority and legitimacy of the state. The combined questions raised by hacking back undermines the viability of the action itself, hacking back is likely to be ineffective and have a negative impact on the development of Internet governance and norms.

Keywords – cyber security, cyber defense, retailation, cyber deterrence, cyber ethics, hack back, intellectual property, cyber theft.

I. INTRODUCTION

In the recent years there have seen several vocal proponents for legalizing corporations to hack back after being targeted by a cyber-attack. As of today, the act of hacking back constitute an illegal action as there is not a legal right to digital self-defense, instead a counterattack is a new perpetrated attack [1, 2].

A strong proponent in the United States has been the Commission on the Theft of American Intellectual Property, a bipartisan commission [3]. The focus for the discussions in the United States has been centered on corporate interests, and the potential loss of intellectual property derived from successful cyberattacks [4, 5]. The Netherlands, France, and the United Kingdom have had similar debates about the future legalization of hacking back. The rationale in Europe has been from a law enforcement stand point instead from a strict corporate outlook. In a European perspective hacking back would allow law enforcement to conduct investigations by hacking into cybercrime perpetrators' computers and networks. The unknown is if hacking back is a viable route to address the problem or if hacking back would trigger new problems and challenges that could lead an entropy in Internet governance and instead delay a formation of regulating cyber norms codified by national legislators and international organizations. Multinational governance entities, such as the United Nation (UN), the International Telecommunications Union (ITU), the European Union (EU), the Internet Corporation for Assigned Names and Numbers (ICANN), work together with national legislators and interest groups to create norms and rules for the Internet and the future utilization of the net. If corporations have a broad mandate to strike back against hackers it is likely dissolving Internet public norms because the driving force is then the best interest of the corporation at the point of corporate decision making. The idea with public Internet norms is to balance private and public interests.

The main question raised in this paper is if legalization of corporate hack back is a viable route – or if the approach is based on weak assumptions. The report from the Commission on the Theft of American Intellectual Property is a central document, due to its acceptance within the corporate and political sphere, and the report advocates hacking back to recover stolen intellectual property and data.

II. GROWING FRUSTRATION

The last decades have seen a shift from cyber criminals to foreign entities [6,7], and increasingly state actors, seeking to gain a geopolitical, military, industrial, competitive, intelligence or commercial advantage. The state actors have access to a variety of options that the earlier cyber criminals did not possess, such as integration to intelligence community, government aligned business interests, and the state sponsored attack are well funded with more resources allocated. The entry of state sponsored attack have increased the targeted states' concerns, even if the targeted states' bureaucracy themselves are not affected but instead their business and society. In an effort to address this new threat, the nation states have pursued cyberdefense abilities.

Several advanced democracies, and their ministries of defense, are creating what they define as cyber warfare units. The question is if these fairly small military cyber defense units will have an impact in a cyber-conflict as these units are to a high degree forensic team seeking attribution and

Kallberg, Jan, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," IT Professional , vol.17, no.1, pp.30,35, Jan.-Feb. 2015
doi: 10.1109/MITP.2015.1

determine vulnerabilities at a limited number of systems and points of entry. It is unlikely that any of the cyber units, by their sheer size and abilities in relation to the infrastructure and economy, will have a measurable influence on the developments of a future cyber interchanges. The main contribution that the state can offer is coordination and direction due to the absence of defensive and even punitive measures from the nation state.

The new militarized cyber units are not able to provide real-time protection or support to the affected corporations nor does any other nation state initiatives provide adequate protection for businesses from mainly state-sponsored attacks. The absence of nation state's ability to protect leads to a growing frustration in the corporate sector.

III. Supported Practices

In the report, the Commission on the Theft of American Intellectual Property recommends three general ways to address the problem. First, that corporate America implement prudent vulnerability-mitigation measure followed by a call for public support for American companies and technology that can both identify and recover IP stolen through cyber means, and finally a recommendation to the legislators to reconcile necessary changes in the law with a changing technical environment [8]. Industrial practices seek to determine the extent of an attack, the intent of the attacker, and create a picture why and how the attack was possible. The aggregated knowledge from forensic and analytic work would then create a set of cyber intelligence enables counter activities [9]. The counter activity is today illegal, even if the corporate ability to trace, attribute, and determine origin of an attack is increasing. The recommendations of the commission would, if becoming law, remove the legal hindrance for corporate cyber-intelligence and penetrating systems on foreign soil as long as there was probable cause that these systems had been engaged to steal American intellectual property.

IV. The Assumptions of Hacking Back

The Commission on the Theft of American Intellectual Property stated in their report released May 22, 2013; *"Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information."* This statement was embraced both by members of Congress and the business community as a major endorsement of a right to strike back. The report was endorsed by Chairman Rogers of the House Permanent Select Committee on Intelligence who released the following statement; *"I heartily agree that Congress and the Administration need to act quickly to help American companies defend the hard work and innovation that is the life-blood of our economy. That must begin with getting cyber information sharing legislation signed into law"* [8].

The question is – what are the endorsers actually proposing and what assumptions is it based upon? The model the Commission on the Theft of American Intellectual Property are proposing would allow corporations to breach foreign systems to repossess stolen intellectual property as long as there is no actual damage. If corporate entities were allowed to hack back and engage foreign entities in cyber-attack exchanges, according to the model proposed by the Commission on the Theft of American Intellectual Property, it relies on several assumptions. These assumptions are also present in other propositions of allowing corporations to hack back, as the assumptions are general, and underlying the general argument.

A. The private companies can attribute.

The idea of legalizing hack back operations is based on the assumption that the defending party is able to attribute the initial attack with pin-point precision. If a defending party is given the right to strike back it is logically based on the assumption that the counterstriker is able to beyond doubt determine which entity was the initial attacker. If attribution is not achieved with satisfactory granularity and precision, a right to cyber counterstrike would be a right to strike anyone based on suspicion of involvement.

Very few, if any, private entities can as of today with high granularity determine who attacked them and are able to trace back the attack so the counterstriker can determine where stolen data is stored. The lack of norms and a right to strike back, even if the precision in the counterstrike is not perfect, would increase entropy and deviation from norms and international governance. An established threshold for what constitutes an acceptable attribution to give access to a right to hack back is legally complicated and becomes if codified unpredictable. Laws that are not predictable tend to create more confusion than clarity.

B. The counterstriking corporations have the ability to engage a state sponsored organization.

The counterstriking corporation are, under the concept of corporate counter cyberattacks, able the handle their adversaries. So if they are assumed to be able to engage any initial attacker, it is assumed that the counterstriking corporation can handle a heavily funded aggressive state-sponsored organization. The counterstriking company would have limited means to before a counterstrike determine the factual size of the initial attacker and the full spectrum of resources available for the initial attacker. A probing counterattack would not be enough to determine the factual size, ability, and intent of the potential adversary. Following the assumption that the counterstriking corporation can handle any adversary is embedded the assumption that there will be no uncontrolled escalation. Edward N. Luttwak once noted that strategy only matters if you have the resources to execute the strategy [10]. Embedded in Luttwak's statement is the

Kallberg, Jan, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," IT Professional , vol.17, no.1, pp.30,35, Jan.-Feb. 2015
doi: 10.1109/MITP.2015.1

general condition that a counter attacker has to be able to engage the full capacity of the initial attacker, if needed, which can be far beyond the ability visualized in the initial attack. If a counter attacker is not able, then the strategy is flawed.

C. The will be no uncontrolled escalation.

One way to compare the concept of corporate counterstrikes is to use the analogy of a bank robbery. The bank is robbed and the police arrive at the scene. The government takes responsibility for the situation and instruct citizens to leave the area. The law enforcement officers seek to peacefully solve the standoff with the bank robbers. The bank robbers have stolen property from the bank account holders and the shareholders of the bank. By using the same logic that supports the legalized hacking back and apply to the bank robbery, then any bank account holder or bank share holder a right to arrive at the scene firing a firearm of their choice at the bank without any considerations of anyone involved, the risk for an uncontrolled escalation, and unnecessary violence. If the situation is framed as a bank robbery it is obvious that a right to fire at the bank robbers would generate an uncontrolled escalation.

If counter cyberattacks are legalized, logically it carries an assumption that there will be no uncontrolled escalation that affects a 3rd party. The counterstriker does not have the control of the situation, once erupted, that uncontrolled escalation can be avoided if it occurs.

D. The whole engagement is locked in between parties A and B with sufficient ability to created an encapsuled deterrence by the initial defender.

If the absence of uncontrolled escalation assumption is the final outcome the question is how is deterrence created that prevents the initial attacker from continuing attacking. The defending party need to be able to counterattack with the magnitude that the initial attacker is deterred from further attacks. If deterrence is established then the digital interchange will cease and the confrontation ends [11, 12]. The key question is how to establish deterrence – and deterring from which array of cyber operations – without causing any damages. If deterrence cannot be establish it would likely lead to escalation or to a strict tit-for-tat game without any decisive conclusion and continue until the initial attacker decides to end the interchange. The Commission on the Theft of American Intellectual Property expressed May 22, 2013; *"Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information."* A counterattack that leaves no damages are unlikely to deterrence theory to create any long-lasting deterrence [13, 14]. So the counterattack itself cannot serve as a deterrent, then deterrence have to be found outside of the interchange, such as financial sanctions by the initial target's government against the initial attacker's organization. These measures leads to an escalation and that the interchange goes beyond the A – B relation.

The report proposes also a threat-based deterrence model. The report states: *"A different concept for security, known as threat-based deterrence, has been identified as a means to protect the most important information in corporate or government networks."* The passage is summarized later in the text; *"In short, it reverses the time, opportunity, and resource advantage of the targeted attacker by reducing his incentives and raising his costs without raising costs for the defender."*

Deterrence is the achieved by deploying so advanced security measures that it is not worth the effort. The reason to hack back was the high geopolitical, competitive, and economic gain for the attacker. If the attacker know that there is a substansial value that can be retrieved behind the deployed threat-based deterrence the attacker is likely resources to nullify the defense effort.

An argument for hacking back was the concern or suspicion that a significant portion of the intellectual property related to the U.S. Air Force fighter project F-35 had been stolen. If that is true, a threat based deterrence designed after the model proposed by the Commission on the Theft of American Intellectual Property would then include cyber defenses that only can be breached after deploying tens of billions of U.S. dollars and these defenses cannot raise the total cost of ownership for the defender's IT systems. From a logical standpoint, deterrence against future attacks is not achieved by the defender following the proposed methods outlined in the report.

E. The initial attacker has no second strike option.

The interchange will occur with a specific set of cyber weapons and aim points. So the interchange cannot lead to further damages. Even if the initial striker had the intent to rearrange the targets, aims, and potential impacts there will be no option to do so. A new set of second strikes would not be an uncontrolled escalation as long as the targeting occurred within the same realm and values as the earlier strikes. The second strike option for the initial attacker could target unprecedented targets at the initial attackers discretion [15, 16]. Instead, it is more likely that the initial attacker has second strike options that the initial target is unaware of at the moment of counterstrike.

F. The counterstriking company has no interests or assets in the intial attacker's jurisdiction.

If a multi-national company (MNC) counterstrikes a state agency or state sponsored attacker the MNC could face the risk of repercussions if there are MNC assets in the jurisdiction of the initial attacker. Major MNC companies have interests, subsidiaries, and assets in hundreds of jurisdictions. The Fortune 500 companies have assets in the

Kallberg, Jan, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," IT Professional , vol.17, no.1, pp.30,35, Jan.-Feb. 2015
doi: 10.1109/MITP.2015.1

US, China, Russia, India, and numerous other jurisdictions. The question is then if MNC "A" counterstrike a cyberattack from China, what will the risks be for the "A" MNC subsidiary "A in China"? Related is the issue if by improper attribution MNC "A" counterstrikes from the US targeting Chinese digital assets when these Chinese assets had no connection with the initial attack, which constitutes a new unjustifiable and illegal attack on Chinese digital assets. The scenarios for different outcomes are complex and can lead to unpredicted casual and collateral events that is likely to hurt international trust and trade. The idea to legalize hack back, and allow corporations to seek their solution to cyber issues, as a temporary bridge until new Internet governance rules and norms are in place, could lead to increased distrust, entropy, and be contra productive to the long term goal of a secure and safe Internet.

G. The duplicated intellectual property is at one location.

Embedded in The Commission on the Theft of American Intellectual Property report May 22, 2013 is a notion that the stolen information can be brought back; *"Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information."*

For a counterstriker the information that has been stolen needs to be stored at one place with no duplications that can dispersed and distributed. The report The Commission on the Theft of American Intellectual Property assumes that the stolen information and intellectual property are stored in a tangible physical form at a given place. It has been stolen from one place and moved to another place where it can be retrieved and brought back. Analogies would be a can of preserved apricots stolen from the pantry of house A and moved to the pantry of house B, where it can be found and brought back to the pantry of house A. An analogy with cash does not work to visualize the intellectual underpinnings of the Commission on the Theft of American Intellectual Property because cash can be other notes and coins than the original and still maintain the same value for the initial owner if brought back.

This assumption also ignores the likelihood that the initial attacker uses backups to store their data so the initial attacker can retrieve the stolen information if lost.

V. The Role of The State

The nation state is based on several institutional pillars. One of these foundations are the state will protect its citizens and dwellers from foreign violence. Historically the citizenry surrenders its interest for violence and give the state the monopoly on violence, under the laws of the land, against protection. The right to hack back is then an acceptance of a nation state failure to protect their citizenry and businesses. The argument for a corporate right to self-defense due to nation state failure and there are no other mechanism in place to defend their assets. Analogies aligned with the right of self-defense would be the right for banks to hire armed guards to protect their money vaults and the right to bear arms for your own protection, which is legal in several countries. Hacking back is different as it not ends with terminating the attack on yourself, but instead it assumes a counterstrike towards the initial attacker. The right of self-defense traditionally ends when the initial attacker's assault is either prevented, stopped, or passed. A second pillar has been the nation state's monopoly of diplomacy and interaction with other foreign state entities. The corporate hacking back will then be engaging foreign entities and conduct aggressive operations in foreign jurisdictions – a role traditionally and by international law only nation states undertakes. The legitimacy and authority of the initial defender's nation states is undermined by corporate hacking back operations [17].

VI. Conclusions

A future legalization of hacking back has several embedded risks for escalation, deterioration of the international system, increased techno-political entropy, and it is likely to work against the establishment of cyber norms. The idea of legalizing is attractive, from a corporate and even political stand point, in a time of growing frustration as it shows that at least something can be done – when industry and politicians demand counter action. The question is at what price – followed by the question if the concept of hacking back is likely to be successful. The notion that hack back can be a policy option is based on several flawed assumptions and unlikely to be a tool to address the issues with an increasing number of cyberattacks.

[1] 18 U.S. Code § 1030, Fraud and related activity in connection with computers. Availble: http://www.law.cornell.edu/uscode/text/18/1030.

[2] Parliament of the United Kingdom, Computer Misuse Act 1990. Availble: http://www.legislation.gov.uk/ukpga/1990/18/section/4

[3] The Commission on the Theft of American Intellectual Property, The IP Commission report. Availble: http://www.ipcommission.org/

[4] J. Westby, Forbes.com, (November 29, 2012), Caution: Active Response to Cyber Attacks Has High Risk. Availble: http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/

[5] C.M. Matthews, Wall Street Journal Online, "Support Grows to Let Cybertheft Victims 'Hack Back". Availble: http://online.wsj.com/news/articles/SB10001424127887324682204578517374103394466.

[6] J. Kallberg and B. Thuraisingham, "State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks", IT Professional vol. 15, no. 3, May 2013, pp. 32-35.

[7] J.Kallberg, and B. Thuraisingham, "From cyber terrorism to state actors' covert cyber operations", in *Strategic Intelligence Management* (ed), Elsevier, 2013.

[8] U.S. House of Representatives, Chairman Rogers Statement on the Report by the Commission on the Theft of American Intellectual Property. http://intelligence.house.gov/press-release/chairman-rogers-statement-report-commission-theft-american-intellectual-property

[9] Mattern, Troy, John Felker, Randy Borum, and George Bamford. "Operational Levels of Cyber Intelligence." International Journal of Intelligence and CounterIntelligence 27, no. 4 (2014): 702-719.

[10] E. Luttwak, *The grand strategy of the Roman Empire: From the first century AD to the third*. Bsltimore, MD: JHU Press, 1979.

[11] J.M. Collins, Principles of deterrence, *Air University Review*, November-December, 1979.

[12] L. Freedman, Deterrence, Cambridge, MA: Polity, 2004.

Kallberg, Jan, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," IT Professional , vol.17, no.1, pp.30,35, Jan.-Feb. 2015
doi: 10.1109/MITP.2015.1

[13] R.H. Reed, On Deterrence, *Air University Review*, May-June, 1975.

[14] E. Sterner, "Retaliatory Deterrence in Cyberspace", *Strategic Studies Quarterly*, Spring 2011.

[15] J. Kallberg and R.A. Burk, Failed Cyberdefense: The Environmental Consequences of Hostile Acts, *Military Review*, May-June 2014, pp. 22-25.

[16] J. Kallberg and R.A. Burk. Cyber Defense as Environmental Protection - The Broader Potential Impact of Failed Defensive Counter Cyber Operations in Conflict and Cooperation in Cyberspace: The Challenge to National Security. Eds. P.A. Yannakogeorgos; A.B. Lowther. Philadelphia: Taylor & Francis, 2013. 265-275.

[17] J. Kallberg, (July 28, 2013), Private Cyber Retaliation Undermines Federal Authority, *Defense News*.