A Critique of Active Defense or 'Hack Back'

Anthony Caldwell[1], Kevin Curran[2]
[1]*Pramerica Systems Ireland Letterkenny, Ireland*
[2]*Computing, Engineering and Intelligent Systems, Ulster University, UK*

Abstract

Beyond the context of "ethical hacking" where network attacks are conducted with the explicit permission of the network owner, such as during a penetration test, "hacking" typically violates state and federal laws. An emergent perspective that a company may take the law into their own hands and fight fire with fire termed 'hack-back' or 'active defense' has begun to gain momentum. This is where a corporate entity may engage in attacks which are commensurate with the attack perpetrated. We explore the emergent area of 'active defense' or 'hack back strategy' where, in response to persistent and potentially damaging hack attempts upon an entity, an active defense model is considered. We outline the cyberdefense team and what this might mean from an active defense perspective.

1. Introduction

Approximately forty percent of the global population were estimated to use the Internet in 2016 [1] rising to approximately sixty percent in 2020 [2]. It may be said that these progressive technological advances have been led by our social need for more interconnectedness, education and business transactions. The integration strategies adopted by corporations and state agencies can expose mission-critical services to cyber threats through exploitation of existing vulnerabilities in those connected networks, thus reducing the organization's overall cybersecurity posture [3]. Of some concern then are governmental reports from the UK indicating that 93% of large organizations have had a security breach in the previous year incurring costs of the order of billions of pounds per annum and increasing [4]. A strategy initiated by the GCHQ termed the Active Cyber Defense (ACD) programme in 2016 [5] was designed to address high-volume attacks affecting the everyday lives of the end user, corporations and state agencies but not the more sophisticated attacks which are dealt with by cybersecurity teams. Sophisticated attacks such as advanced persistent threats (APT) led to technological safeguards and security awareness programs working in concert to model the defense in depth approach. But, while such techniques as embedding electronic watermarks, user awareness programs and instituting 'honey pots' to attract and trap the hacker, technology continues to outpace most of our efforts in industry.

Even the legal frameworks in place to deal with such threats are limited. It is the globally decentralized architecture of the Internet which facilitates cyberattacks which [6] argues the case for the hack back strategy through the lens of the international law and coins the term 'transboundary cyberharm'. The problem becomes more acute when we combine the growing use of cloud computing, IoT and edge computing with our insatiable need for mobile devices further complicating the threat landscape both technically and legally. Cyberattacks have many goals; denial of service, vandalism, hacktivism, identity theft and financial gain to name a few and the Computer Fraud and Abuse Act in the United States (18 U.S.C. 1030, et. seq.) lays down a framework for how unauthorized access to computers may be prosecuted. Although jurisdictional variations exist worldwide, hacking a computer or network is illegal, regardless of intent. There are due diligence obligations regarding transboundary harm arising from evolving international laws [7, 8]. Developing appropriate legislation, strategies, and regulatory frameworks act to support what must happen when faced with non-state actors [8]. It is important to recognize technical and economic gaps in development among states makes international co-operation essential and the area transboundary harm an increasingly developing concept.

Beyond the context of "ethical hacking" where network attacks are conducted with the explicit permission of the network owner, such as during a penetration test, "hacking" typically violates state and federal laws. An emergent perspective that a company may take the law into their own hands and fight fire with fire termed 'hack-back' or 'active defense' has begun to gain momentum [6]. This is where a corporate entity may engage in attacks which are commensurate with the attack perpetrated. It is the central focus of this paper to highlight the issues with this and offer some guidance on what might be an appropriate strategy to consider before engaging in this activity. The main contribution is to demonstrate how to construct the technical and legal frameworks necessary to mitigate transboundary cyberharm from active defense.

2. Literature Review

The GCHQ state that *'It is not intended to imply retaliation ("hack back") by victims or militarisation*

of the internet – in this case "active" means getting off our backside and doing something, rather than any of the more esoteric definitions.' [5]. This seems to suggest a fight rather than flight posture. However, is there a clearly definable legal or technical boundary to a corporate network? It would seem that this is not as distinct as previously thought with considerable collateral damage likely if an otherwise innocent intermediate server location is used as the battleground. If we return to those engaged in the increasingly popular cloud-based solutions, this problem becomes ever more complex since the origination of the attack may be from a victim's location, unaware of their vulnerabilities and in close proximity to others in the cloud thus exposing the many more to attack. Given that the theatre of conflict is global, there is no flight and the risk may lie in adopting a stance that there is only fight. In fact, so tempting is the hack back strategy that the Obama administration commission on the theft of American intellectual property gave serious consideration to the hack back strategy [9]. To this end, considerable care is warranted in those cases where a corporate entity engages in a cyberwar with the indistinct, globally distributed, technically adept cyberwarriors who are experts at obscuring their locations and attacks behind the innocent. Be under no illusions, the cost of the hack back strategy will be high and it is important to reflect on what this may mean. With the advent and rapid adoption of cloud computing, many of the traditional responsibilities of organisations in terms of configuring, maintenance of their infrastructure has shifted from clients to cloud providers to the internet of things (IoT). From the users' perspective, the location, equipment or configuration of their resources and data are not necessarily known.

In cloud computing the user is provided with a 'virtualised' computer resource hosted at the cloud vendors site [10]. The attractiveness of instant availability to resources and information sharing seem, superficially at least, to be beneficial. Organizations only pay for services when they are required. Applications may be accessed by various means and devices or through web browser. Overall, cloud computing offers lower total cost of ownership. Such is the trust level of the cloud that 75% of IT professionals view the public cloud as more secure than their own data centers [11]. However, the significant security vulnerabilities noted by security experts are difficult to ignore such as, large-scale cloud facilities without sufficient redundancy systems in place represent a single point of failure when we consider the availability and confidentiality of corporate data [12], data loss and leakage (67%), threats to data privacy (61%), and breaches of confidentiality (53%) [13]. As regards some general strategies when considering cloud computing services, it is generally recommended that data is encrypted before storing it in the cloud to ensure that the cloud service provider has clear security measures in place for back-up and failover [14, 15]. Of some concern is the 'separation between nodes' problem which has evolved as a point of contention for the cloud provider as well as a point of entry for the would-be hacker. Traditionally, a dedicated hosted environment is used by the corporation where a potential attacker from must negotiate an outer firewall to reach various application and web servers. In cloud computing, all the systems within the 'virtualised' network are in close proximity to other nodes. This means the software that restricts access between nodes becomes pivotal. Instead of facing an infrastructure based on separate physical boxes, an attacker can now purchase a cloud node from the same provider as used by the organisation they wish to compromise, the malicious attacker then begins to craft an attack from their own node, typically present on the same physical machine with similar resources as used by the target organisation. This means more focus on encrypting data wherever it flows, rather than just protecting the device or the network [14]. Since the data and the hardware that hosts the data may be in a cloud environment the risks of active defense become more complex. Where is the cloud service located, if the active defense is to implement a DDoS attack, can we be sure that it can be contained? This is exasperated by the current demand for devices to be online in the new Internet of Things (IoT) era.Kevin Ashton's presentation in 1999 coined the term internet of things (IoT) to describe the convergence of multiple technologies, a network of smart devices which would coordinate the technical updating and usage of the device seamlessly [16]. Think about the 'smart home' which assists the consumer with their energy usage by automatically ensuring lights and electronics are turned off when not in use. The Internet of Things (IoT) is often hailed as offering the ability for consumers to interact with nearly every appliance and device they own [14] thus transforming real world objects into smart objects connected via the Internet [17]. This has seen advantages in environmental industries as regards clean water and air or indeed medicine sensor-equipped shirt that monitors a patient's vital signs [14]. Within the internet of things must come the security of the internet of things also. In this respect, the 2020 Unit 42 IoT Threat Report from Palo Alto noted that 98% of all IoT device traffic is unencrypted, 51% of threats for healthcare organizations involve imaging devices and 72% of healthcare VLANs mix IoT and IT assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network [12]. This would seem to suggest that there are weak device and network security protocols in place giving attackers the opportunity to compromise IoT systems. Couple this with IoT trends which are looking towards cloud computing as an analytic and storage requirement, there is a risk that even the big-data analytics prized by many could be compromised. In order to engage in 'active defense' a corporate entity needs to be sure that it has created the necessary protections for themselves and that collateral damage is controlled.

3. Corporate Responsibility

Corporate policies are needed to address emerging technology threats. Not having clear standards in place opens the door to risks when we consider the increasing availability of commercial mobile IT from which many threats exist, according to recent reports [18]. Unfortunately, companies have been slow to create and implement policies that address the many mobile technologies that are increasingly becoming part of the workplace. A clear, well-communicated policy and standards set boundaries for employee while at the same time mitigating against any violations of corporate responsibility and accountability. As with any new policy, user awareness is key particularly in relation to accessing data in the corporate network, sharing, storing and transferring critical files on employee-owned or corporate-provisioned devices. Within the context of ethical hacking which is regularly carried out by trained cybersecurity professionals, network attacks are conducted with the explicit permission of the network owner, i.e. the penetration test. At a strategic level, malicious hackers may be supported by a nation-state making identification of the actor difficult using standard tactics, techniques and procedures. Typically, the technical means for attribution/identification of an actor involves the analysis of network traffic to determine the final source of the attack. Tools like Wireshark to map the paths between computer hosts towards suspicious IP addresses [10]. Issues with attribution such as this then come into play. Local law enforcement hopefully have the capability and capacity to investigate the incident, if not because of requisite skills or an excess of higher priority cases an enterprise may still have interest in learning the source of the attack in order to pursue legal action in civil court. However, if an enterprise that conducts attack or carry out activities against a computer or network outside the U.S. they are then subject to the laws of that country. Although defense may be passive and attack more active, the latter increases capacity to make war; the former does not. The defensive form of warfare is intrinsically stronger the offensive. For example, the defender benefits from knowledge of the terrain, since the strength and direction of attack comes from in-depth knowledge of the paths to the defenders position. However, while an active physical war sees advantages in being able to map hidden paths to the opponent, not so in cyberwarfare. In cyberwarfare the available paths to a victim, both hidden and in full view, are not so clear. The job of the cybersecurity professional is to ensure that vulnerabilities are identified and remediated as quickly as possible but to also be fully aware that all that is required for an attacker to gain a foothold in a victim's computer or network is one access point, be it technical or social. On an internal network or intranet, there is limited access and limited numbers of employees. However, this becomes all the more difficult when externally facing companies and state agencies operate in full view of the public. Ultimately, corporate responsibility begins and ends with their own internal security procedures to deal with cyber-attacks and many contemporary firms have employed the use of information security experts, in the formation of cyberdefense teams. [19] considers the importance of such internal self-defense perspectives i.e., security within one's own network. For example, the honeypot strategy is designed to attract the malicious actor inside the defender's own system to observe their techniques. These techniques (signatures) then form part of an intelligence profile used to screen or block incoming traffic associated with those threat indicators. This is typically automated and facilitated by intrusion detection systems (IDS) and web application firewalls (WAF) acting in concert. A combination of corporate security polices, the aforementioned intrusion detection systems, user awareness programmes and the cyberdefense team, forms the well-known 'defense in depth' model. a one-to-one exercise, where an organization deploys specific technologies to counter an equivalent risk. This is a holistic approach to protect all assets, with respect to interconnections and dependencies using an organization's available resources to provide effective layers of monitoring and protection. This involves employing multiple technical, governance and behavioural mechanisms to protect a company, application or critical infrastructure. This would include, but limited to, patch management on a regular basis, red-team exercises, compliance with current standards and policies in the industry and user awareness programs. But in cyberwarfare where active defense may be employed, a different stance is taken.

4. Recommendations

In the active defense model, we are now beyond the boundaries of the defender's network where payloads may be used to take action against the malicious actor identified as the cause of harm to the corporate or state agency. There are passive versions of active defenses that can allow the collation of information that is non-interventional such as networks sniffing which monitors traffic but does not necessarily intervene and send malicious data. This might also involve, scanning and enumeration of web pages for valuable data and would typically have the least impact on other users' computers. However, the interventionist attack might take the form of the enterprise conducting a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack on the server hosting the website as the source of a data breach set up with the intent of publicizing embarrassing or sensitive data. [10] points out the problematic nature of this from the perspective of proportionality of attack meaning the effect on the attacker's system must be proportional to the effect desired by the enterprise. It is emphasized that while care must be taken to not to

cause harm to a third party, legal protection is difficult to secure e.g., trade secret theft.

From 2015 the GCHQ has sought to address cybersecurity harms in an interventionist manner in an effort to actively reduce online harm to UK citizens and businesses [20]. However, can a nation state or enterprise conduct such attribution without exposing itself and its leadership to civil and criminal liability as well as reputational damage? Most notably in the US, there is the Wiretap Act (18 U.S.C. §§ 2510-22, also known as "The Act," or "Title III of the Omnibus Crime Control and Safe Streets Act of 1968") prohibiting unlawful interception of wire, oral, or electronic communications. Any public identification of alleged hackers should be avoided since this may trigger laws concerning defamation of character and violation of privacy points out [10]. The crime needs to be attributed to a specific actor and a target for the civil suit. [20] urge caution and consultation with lawyers prior to attacking a hacker's computer or network. [10] recommends that a policy surrounding attribution be written and clarified before any active defense posture be taken ensuring that access to a malicious actor's computer is limited to the minimum amount needed to attribute the source of the attack. For example, if entry has been gained to a malicious actor's computer data may be exfiltrated that is unrelated to the original attack on the enterprise. Consider that the malicious actor is using the industrial control systems of a hospital or power plant, a misguided active retaliation could trigger a major catastrophe [21].

5. Discussion

Cyberdefense teams are cognizant of the operational technologies that support the critical infrastructure of their industries, from manufacturing, transportation, payroll and communications, all of which are heavily dependent upon information systems for their monitoring and control. While "security through obscurity" concept generally works well for environments with no external communication connections, the active defense model goes beyond this to become an actor outside the perimeter walls and DMZ and thus brings legal issues as noted above. Some legal protection may be afforded by posting warning banners, but no guarantee of insulation [10]. There is no shortage of high-profile data breaches and there may be some degree of active defense but staying within the boundaries of the law, but laws change with context and in some cases public opinion. On this basis, cyberdefense teams considering active defense, need to include legal representation into their teams to protect themselves, the organization and perhaps the target of the active attack. How do we construct the technical and legal frameworks necessary to mitigate transboundary cyberharm from active defense? Where a corporate entity engages in a cyberwar with a globally distributed cybercrime network, their locations and attacks may originate behind the cloak of an innocent party. In military planning terms, the purposes of active defense can be thought of in terms of constraints (things the organization must do), while prohibitions can be thought of as restraints (things the enterprise must not do) [22]. As regards the cloud, many presentations on cloud computing began with its definition, but they predicted that cloud computing would just become another avenue for data storage and transmission [14]. A complete security solution for cloud computing is still in development, so at present, any migration to cloud computing carries risk [10]. It would appear from the security perspective at least that the adage of caveat emptor may be the wisest policy to adopt despite the lofty promises of these cloud computing firms.

Cloud computing is in rapid development and as yet, the research from either industry or academia on the specific threats is still very new. So how can an organisation confirm whether a cloud service provider is up to scratch? The common assurance maturity model (CAMM) may help the small to medium business. This model offers guidance on the levels of security cloud computing companies provide which may have benefits for both purchaser and supplier. The model essentially leads to the development of a global repository where organisations may share their information assurance maturity based upon the services they provide [23]. In simple terms, think of this model as a rating system where five stars represents high quality and one star represents lower quality. Importantly, the model utilizes the ISO 27001, COBIT and PCI DSS standards for data as a reference point for potential consumers to consider. However as with any new model, over-simplification of the measurement scales can be problematic.

"No one starts a war- or rather, no one in the right senses ought to do so- without being first clear in his mind what he intends to achieve by that war and how he intends to conduct it. The former is its political purpose; the latter its operational objective" [24]. It may not be possible to conduct a cyber war, to enact it in such a way as to make it an extension of corporate policy, to overcome the enemy and make them comply with your will (policy). For as tempting as the hack-back strategy is, unintended and potentially harmful consequences are possible. Consider for example a compromised hospital server which is used as the staging point for a denial of service attack against a major retailer, government body or financial institution. Hack-back, without due consideration may only see the compromised server and engage in aggressive tactics to shut the attack down regardless of the server's main function. Essentially, this runs the risk of collateral damage being extensive. In this respect, proportionality is key if considering active defense, meaning the effect on the attacker's system must be proportional to the effect desired by the state agency or enterprise. For example, upon detection of

a threat from an attacker, a redirection would be safer and implemented so as to cause little harm.

6. Conclusion

There is a growing movement within the network security field of active network penetration testing which sometimes blurs the boundaries between what is legal and what is illegal. Organizations are aware that they can take part in attacks which are commensurate with the attack perpetrated. This paper explored the emergent area of 'active defense' or 'hack back strategy' where, in response to persistent and potentially damaging hack attempts upon an entity, an active defense model is considered. We outlined the cyberdefense team and what this might mean from an active defense perspective.

7. References

[1] Internet Live Stats (2016). http://www.internetlive stats.com/internet-users/, (Access Date: 06/02/2018).

[2] Statista (2020). https://www.statista.com/statistics/ 617136/digital-population-worldwide/ (Access Date: 22 February 2021).

[3] 18 U.S. Code § 1030. Fraud and related activity in connection with computers. http://www.law.cornell.edu/ uscode/text/18/1030, retrieved 06/02/2018. (Access Date: 22 February 2021).

[4] GovUK (2013). 2013 Information Security Breaches Survey. https://www.gov.uk/government/publications/ information-security-breaches-survey-2013-technical-report, retrieved 06/02/2018. (Access Date: 22 February 2021).

[5] Levy, I., (2018). Active Cyber Defense – One Year On. https://www.ncsc.gov.uk/information/active-cyber-defense-one-year (Access Date: 22 February 2021).

[6] Messerschmidt, J., (2013). Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm. Columbia Journal of Transnational Law, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2309518.

[7] Dörr, O. (2015). Obligations of the State of Origin of a Cyber Security Incident. German Yearbook of International Law 58, pp.85-99.

[8] Takano, A., (2018). Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications. Laws, MDPI, Open Access Journal, Vol. 7, Issue. 4, pp. 1-12.

[9] Economist, The (2013). Fighting China's Hackers. Available at http://www.economist.com/news/united-states/21578405-it-time-retaliate-against-cyber-thieves-fighting-chinas-hackers, retrieved 05/02/2018.

[10] Jarko, C., (2014). Finding the Fine Line Taking an Active Defense Posture in Cyberspace without Breaking the Law or Ruining an Enterprise's Reputation. The Sans Institute. Available at: https://www.sans.org/reading-room/whitepapers/legal/paper/36807 (Access Date: 22 February 2021).

[11]. Oracle (2020). Oracle and KPMG Cloud Threat Report 2020. https://www.oracle.com/ie/cloud/cloud-threat-report/ (Access Date: 22 February 2021).

[12] Palo Alto Networks (2020). 2020 Unit 42 IoT Threat Report. https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (Access Date: 22 February 2021).

[13] Cloud Security Insiders (2018). Cloud Security Report. https://www.cybersecurity-insiders.com/portfolio /download-cloud-security-report/ (Access Date: 22 February 2021).

[14] Curran, K., (2018). Security and the Internet of Things in Cyber Security: Law and Guidance Handbook, Bloomsbury Publishers, London, UK. pp: 371-382, ISBN: 978-1-52650-586-6.

[15] Cocking, S., (2019). 7 Trends to Watch in IOT and Cybersecurity in 2020. https://irishtechnews.ie/7-trends-to-watch-in-iot-and-cybersecurity-in-2020/ (Access Date: 22 February 2021).

[16] Elder, J. (2019) How Kevin Ashton named the Internet of Things. Avast News. 20 August 2019, https://blog.avast.com/kevin-ashton-named-the-internet-of-things (Access data: 23 February 2021).

[17] Fathi, A., Curran, K. (2017). Detection of Spine Curvature using Wireless Sensors. Journal of King Saud University – Science. Vol. 29, No. 4, October 2017, pp: 553-560, Elsevier, ISSN: 1018-3647, DOI: http://dx.doi.org/10/1016/j.jksus.2017.09.014 .

[18] Finkle, J., Chatterjee, S., Maan, L., (2014). EBay asks 145 million users to change passwords after cyber-attack. Reuters. http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521, (Access Date: 08/01/2018).

[19] Rosenzweig, P., (2014). International Law and Private Actor Active Cyber Defensive Measures. Stanford Journal of International Law, Vol. 50, No. 2, pg. 103-109.

[20] Strand, J., Asadoorian, P. (2013). Offensive Countermeasures: The Art of Active Defense. Rapid City: CreateSpace Independent Publishing Platform; 2 edition.

[21] Levy, I., (2019). Active Cyber Defense - The Second Year. https://www.ncsc.gov.uk/blog-post/active-cyber-defense--acd---the-second-year (Access Date: 22 February 2021).

[22] US CERT (2016). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Available at, https://us-cert.cisa.gov/sites/default/files/recommended_practices/ NCCIC_ICS-ERT_Defense_in_Depth_2016_S508C.pdf (Access Date: 22 February 2021).

[23] Rubino, F. E. (2015). Frequently Asked Questions About International Crime.https://www.frankrubino.com /International-Law/International-Crime-An-Overview.shtml (Access Date: 22 February 2021).

[24] Von Clausewitz, C., (1832). On War, Everyman's Library. ISBN: 1-85715-121-6.

