Politeja
No. 6(93), 2024, pp. 135-160
https://doi.org/10.12797/Politeja.21.2024.93.06

Dominika DZIWISZ
Jagiellonian University
dominika.dziwisz@uj.edu.pl

LEGALISING FORMS OF ACTIVE CYBER DEFENCE (ACD)

THE THEORY AND PRACTICE OF PRIVATE CYBERSECURITY PROVISIONING

ABSTRACT The article analyzes the legality and implications of active cyber defense (ACD), including the controversial practice of retaliatory hacking (hack-back), by private entities. The author presents the current legal restrictions in the United States, where companies are essentially barred from taking aggressive defense measures beyond their own networks, despite growing cyber threats. The paper discusses the arguments for and against legalizing ACD, including issues of attack attribution, company readiness, the risk of escalating international conflicts, and potential legal consequences. The article focuses on legislative proposals, such as the Active Cyber Defense Certainty Act, aimed at mitigating these restrictions, while pointing out the associated challenges and dangers.

Keywords: cybersecurity, active cyber defence, ACD, hack-back

INTRODUCTION

Former FBI Director Robert Mueller once said that there are only two categories of companies: *...those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.*[1] Amid rising tensions in international relations, the world is witnessing unprecedented levels of interconnectedness and complexity, partly driven by the internet. For private companies, this has at least two key implications: firstly, international business leaders are increasingly vulnerable to global risks; secondly, conventional approaches to mitigating such risks are falling short. In a survey conducted among risk management experts in late 2022, cyber incidents such as cybercrime, IT failures or outages, data breaches, fines and penalties emerged as the primary risk confronting global businesses in 2023.[2] Consequently, private sector entities find themselves on the front lines of cyber conflict, grappling with various hostile actors aiming to steal and exploit their intellectual property, undermine their infrastructure and disrupt their operations. Furthermore, private firms function not merely as 'objects', but also as 'agents' of cybersecurity. In essence, they require safeguarding while also offering protection to other companies, occasionally fulfilling both roles simultaneously.[3]

As analysed by Patrick Lin, the realm of cybersecurity evokes a profound sense of vulnerability, wherein individuals often find themselves in a situation of solitary defence. Lin underscores the absence of traditional safeguards, which are akin to state-guarded borders or neighbourhood police surveillance in the cyber domain, where individuals assume the primary responsibility for safeguarding their information and communication technologies. Furthermore, the assistance provided by national security institutions may not be sufficient.

Joseph Bonavolonta, an Assistant Special Agent in charge of the FBI's 'Cyber and Counter-Intelligence Program', acknowledges this candidly: *In all honesty, we [FBI] frequently recommend that individuals simply comply with the ransom demands.*[4]

By 2005, passive defence was considered inadequate in cyberspace as it enabled attackers to operate with minimal perceived risk. This imbalance favoured the attackers and led to dual financial burdens for companies, which had to cover expenses for both defensive technologies and the consequences of successful attacks.[5] Cybersecurity

1 R.S. Mueller III, "Combating Threats in the Cyber World," *Federal Bureau of Investigation*, 1 March 2012, at https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies, 12 January 2024.

2 J. Rudden, "Business Risks Globally 2020," *Statista*, 22 August 2023, at https://www.statista.com/statistics/422171/leading-business-risks-globally/, 14 January 2024.

3 J. Pattison, "From Defence to Offence: The Ethics of Private Cybersecurity," *European Journal of International Security*, vol. 5, no. 2 (2020), p. 237.

4 S. Berinato, "Active Defense and 'Hacking Back': A Primer," *Harvard Business Review*, 21 May 2018, at https://hbr.org/2018/05/active-defense-and-hacking-back-a-primer#:~:text=%E2%80%9CThis%20is%20a%20moment%20when, 15 December 2023.

5 M. Christen, B. Gordjin, M. Loi, *The Ethics of Cybersecurity*, Cham 2020.

experts have criticised the practice of relying solely on passive defences as ineffective, comparing it to outdated 'duck-and-cover' strategies during nuclear threats. Instead, they advocate for a more active approach, suggesting the need to counter cyberattacks with proactive measures.[6] A policy brief from the Center for North American Security argues that: *Passive defenses are a necessary component of a well-designed cyber defense program, but they are no longer sufficient to address increasingly sophisticated threats.*[7] Given the continual increase in cyber threats to companies, it is highly probable that they will be granted additional cybersecurity powers in the long run. Currently, despite this stark reality, response options to an attack within the private sector remain outdated and limited. The prevailing approach is predominantly reactive, which provides an advantage to the attacker. To defend their networks, companies primarily rely on passive measures such as firewalls, intrusion detection and prevention systems (IDS/IPS), data loss prevention (DLP) technologies, malware protection systems and regular software patching.[8] When hackers breach these defences, companies have few recourse options, as recovering lost data before it is sold or exploited is seldom feasible.

In the United States, existing federal legislation prohibits private entities from adopting more aggressive self-help approaches or seeking assistance from the commercial cybersecurity market.[9] Therefore, private enterprises are increasingly advocating for the implementation of retaliatory cyber measures, often referred to as 'active cyber defence' (ACD) or, more assertively, 'hack-back', as a means of deterring and safeguarding themselves against attacks. Consequently, the debate surrounding ACD unfolds simultaneously within academic circles and broader political discussions concerning the privatisation of security. Proponents often draw parallels between these actions and the right of self-defence in discussions regarding the authorisation of private sector actors to retaliate through hacking activities. Conversely, opponents of private sector hack-back initiatives tend to equate such actions with vigilante activities in the physical sphere, which encompass enforcement, investigation and punishment in the absence of legal law enforcement authority. Therefore, the central theme of this discourse revolves around whether victims of cybercrime in the private sector should, under specific circumstances, be capable of retaliating against attacks extending beyond their internal networks. Capabilities such as these have, to date, been exclusively reserved for law enforcement agencies, notably the FBI. Legislative proposals such as the Active Cyber Defense Certainty Act (ACDC) aim to eliminate this restriction, empowering private companies to implement aggressive cyber defence measures. These measures would not

6 S. McGee, R.V. Sabett, A. Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law*, vol. 8, no. 1 (2013), p. 12, at https://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3/, 10 January 2024.

7 I. Lachow, "Active Cyber Defense: A Framework for Policymakers," *Center for a New American Security*, 22 February 2013, at https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers, 10 January 2024.

8 R.M. Lee, *The Sliding Scale of Cyber Security: A SANS Analyst Whitepaper*, August 2015, at https://perma.cc/TU3K-XEFU, 10 January 2024.

9 D. Broeders, "Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?," *Journal of Cybersecurity*, vol. 7, no. 1 (2021).

only facilitate the identification of attackers, but also potentially allow for the removal of compromised data, even beyond their immediate networks.

The discussion regarding private ACD has become particularly significant following the announcement (by the Biden administration) of a new 'National Cybersecurity Strategy'.[10] This strategy calls upon America's tech industry and software makers to assume greater responsibility for safeguarding their systems. It acknowledges the crucial importance of strong collaboration between the public and private sectors in securing cyberspace and recognises that the current approach of primarily relying on voluntary cybersecurity efforts is inadequate. While the solutions proposed by Biden are both rightful and necessary, the government is once again placing responsibilities on the private sector without allowing for more assertive actions to be taken. Furthermore, the Biden administration has taken a clear position, cautioning private digital defenders not to retaliate against cyber attackers amidst a surge of breaches affecting American businesses and citizens. Ambassador-at-large for Cyberspace and Digital Policy, Nathaniel C. Fick, stressed the importance of the U.S. government maintaining exclusive authority over the legitimate use of force in American society to prevent the digital realm from descending into vigilantism. Moreover, he highlighted the importance of companies refraining from initiating conflicts that fall within the purview of government, underlining a clear boundary that should not be crossed.[11] It is possible that, for many years, the government has consistently assumed that in cybercrime, cyber espionage and cyber warfare the role of the private sector is limited to being a victim and reporting crimes committed. There is a significant gap between the actions we would expect from businesses to secure themselves against attacks and what the government imposes on them.[12]

The potential benefits of allowing private companies to engage in active cyber defence (ACD) must be weighed against the risks. Therefore, this article examines the key issues and challenges involved in expanding the authority of private companies to participate in new forms of ACD. The argument posits that although the potential defensive advantages and other benefits of private-sector armaments are substantial, the risks to defenders, innocent bystanders and international conflict stability might be markedly higher. However, the article refrains from taking sides in the debate, considering that at a time when we require additional response options to address cyber threats, and while we are still grappling with conceptualising the cyber domain, it might be premature to dismiss reasonable options.

The selected case studies are ACD proposals for private companies within the United States, which uniquely offer a national context in which there is a relatively open debate on this issue. The abundance of resources from U.S. think tanks, security firms and government entities allows for a thorough analysis. The research hypothesis posits that while the private sector's implementation of some solutions in the realm of cyber

[10] "National Cybersecurity Strategy," *White House*, March 2023, at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 12 January 2024.

[11] Ibid.

[12] J. Healey, *Shaping American Cyber Security Policy*, interview by D. Dziwisz, November 2013.

self-defence is necessary, it is essential to clearly delineate the boundary between government and private entities regarding applied cybersecurity solutions. The sponsors of the Active Cyber Defense Certainty Act and others have suggested measures that exhibit excessive openness, as ACD legislation ought to uphold the principle that the approval of law enforcement agencies is granted on a case-specific basis. The capacity of federal authorities to grant authorisation and exercise rigorous supervision over corporate involvement in defensive cyberattacks is poised to alleviate the concerns surrounding a perceived 'wild west' scenario, wherein the private sector might engage in unbridled hack-back activity against any entity.

This paper will unfold as follows:

– Part 1 serves a definitional purpose. Given the lack of a universal definition of ACD, an explanation of the usual categorisation of passive and active defence is provided. Clear distinctions are drawn between passive defence, active defence and the most controversial form – hack-back;
– Part 2 focuses on the current state of affairs in the USA. It presents the political discourse surrounding the implementation of ACD, with particular attention given to the ACDC Act – which revitalised widely discussed controversies and dilemmas associated with legalising ACD for the private sector;
– Part 3 delves into the security risks of legalising private ACD, divided into three fundamental problems: the incorrect attribution of an attack; the lack of preparedness of private firms to implement ACD; the potential international consequences of employing private ACD.

DEFINING PASSIVE DEFENCE, ACTIVE DEFENCE AND HACK-BACK

'Active defence', or 'offence-as-defence',[13] is not a new term within national security. In the United States, it started to gain traction in the 1970s during discussions regarding a defensive strategy centred on mobility. This approach sought to tire out an attacker by consistently engaging them with strong combined weapons teams and task forces operating from mutually supported battle positions across the battlefield.[14] Despite the controversy and heated debate around this approach, defenders' ability to achieve mobility hinged on them being able to utilise military intelligence and indicators in order to do the following: (1) proactively identify threats (the early detection allowed for timely responses); (2) react to attacks within the designated defensive zone or contested area; (3) neutralise enemy capabilities within the contested area, but avoid targeting the adversary directly.[15] In the original sense, active defence techniques granted

[13] L. Kello, "Private-Sector Cyberweapons: Strategic and Other Consequences," *SSRN Electronic Journal*, 2016, pp. 1-24.

[14] "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," *Center for Cyber and Homeland Security*, October 2016, p. 6, at https://perma.cc/SAX8-4LW3, 10 August 2024.

[15] Ibid.

the defender the capacity to swiftly adjust to the environment in real-time, enabling the proactive handling of attacks. In contemporary terms, according to the definition given in the Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, active defence refers to *utilizing limited offensive measures and counterattacks to prevent the enemy from gaining control over a contested area or position.*[16] In contrast, passive defence comprises *actions aimed at decreasing the likelihood of and mitigating the impact of damage resulting from hostile actions without the intent of initiating them. See also: active defense.*[17] Although both of these definitions are common in the military, they were developed at a time when cybersecurity was not a concern.

In February 2011, the then-Deputy Secretary of Defense, Bill Lynn, declared that: *It is insufficient to depend solely on passive defenses that react only after an incident has occurred. We have devised and are now employing a more proactive approach to cyber defense.*[18] This statement heralded changes in American cybersecurity policy, which were subsequently articulated in the Department of Defense (DoD) Strategy for Operations in Cyberspace released in July 2011. The strategy defined 'active cyber defence' in these terms:

(...) DoD's synchronised, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, the DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.[19]

The Center for Cyber and Homeland Security offers a practical framework for developing active defence strategies and presents a set of policy recommendations applicable to both public and private sectors.[20] 'Active defence' is defined by the aforementioned Center as a spectrum of proactive cybersecurity measures situated between traditional passive defence and offence. These measures encompass two main categories: the first involves technical interactions between defenders and attackers, while the second encompasses operations that enable defenders to gather intelligence on threat actors and indicators across the internet. It is essential to note that the term 'active defence' should not be confused with 'hacking-back' – they are not interchangeable. Robert Dewar posits a nuanced definition of ACD that effectively distinguishes it from passive cyber defence approaches by highlighting several key differentiators. It is *an*

[16] United States Department of Defense, *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02*, November 2010, at https://irp.fas.org/doddir/dod/jp1_02.pdf, 6 March 2025.

[17] Ibid.

[18] W.J. Lynn III, "Remarks on Cyber at the RSA Conference," *U.S. Department of Defence*, 15 February 2011, at http://www.defense.gov/speeches/speech.aspx?speechid=1535, 12 January 2024.

[19] United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, p. 7, at https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, 19 January 2024.

[20] "Into the Gray Zone...".

approach to achieving cybersecurity predicated upon the deployment of measures to detect, analyze, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources to take proactive or offensive action against threats and threat entities, including action in those entities' home networks.[21]

Active cyber defence is typically characterised as encompassing proactive measures aimed at safeguarding against malicious cyber activities or cyberattacks, as well as the capacity for real-time detection, analysis and mitigation of threats.[22] One of the most widely accepted definitions, proposed by Paul Rosenzweig, provides a preliminary understanding: *...the synchronized, real-time capability to discover, detect, analyze, and mitigate threats. Active cyber defense operates at network speed using sensors, software, and intelligence to detect and stop malicious activity ideally before it can affect networks and systems.*[23] Other attempts to define active cyber defence focus on strategies aimed at identifying perpetrators and neutralising their ability to either persist with an intrusion or launch future attacks.[24] While they share common attributes – such as: (1) prioritising the utilisation of particular tools to mitigate the immediate repercussions of a cyberattack within target networks; (2) fostering capabilities for direct engagement with perpetrators within their networks; and (3) involving some form of interaction with an adversary, whether direct or indirect – none of the definitions establish clear boundaries or identify which active cyber defence measures are legally permissible.[25] Stated differently, the absence of consensus on the exact parameters defining active cyber defence measures has created extensive difficulties in categorising and characterising different options as lawful or unlawful under international law (especially the Council of Europe's Convention on Cybercrime, commonly known as the 'Budapest Convention on Cybercrime').[26] In this regard, Alexandra Van Dine's division of types into three categories is useful: measures can be passive, active-passive and active.[27] The first category involves no external action and is implemented internally on an entity's network. The second consists of measures deployed on an entity's network, with occasional external

[21] R.S. Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence," in *2014 6th International Conference on Cyber Conflict (ICCC)*, Tallinn 2014, pp. 7-21; after: W. Hoffman, A.E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, Washington, D.C. 2017, at https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf, 6 March 2025.

[22] R.S. Dewar, "The 'Triptych of Cyber Security'..."; A. Van Dine, "When Is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention," *Chicago Journal of International Law*, vol. 20, no. 2 (2020), pp. 530-564, at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1777&context=cjil, 19 January 2024.

[23] P. Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law*, vol. 47, no. 2 (2013), pp. 1-13.

[24] R.S. Dewar, *CSS Cyber Defence Trend Analysis 1: Active Cyber Defense*, Zürich 2017, at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-03.pdf, 2 January 2024.

[25] Ibid.

[26] A. Van Dine, "When Is Cyber Defense a Crime?..."; R.S. Dewar, *CSS Cyber Defence...*

[27] A. Van Dine, "When Is Cyber Defense a Crime?...".

consequences. The third comprises active defence measures that are entirely external to the network and are targeted and deployed specifically to terminate an attack or intrusion. Therefore, international law has distinct implications for each of these categories. In other words, the term 'active cyber defence' is so broad that it is challenging to classify specific actions as legal or illegal.

The term 'active cyber defence' often evokes the notion of initiating counterattacks against adversaries and, in some circles, generates significant opposition to considering ACD a legitimate private sector practice. Simply put, ACD utilises passive, tried-and--trusted methods as a foundation. However, rather than merely reacting to a completed attack or constructing an ineffective barrier in an attempt to deter attackers, it detects, redirects, actively engages and responds to attacks.[28] In practice, this term encompasses both aggressive cyber retaliation measures, which involve retaliatory, disruptive or even destructive responses against an attacker and relatively innocuous actions such as setting up decoy targets – commonly known as 'honeypots' – within a defender's network. It also includes beacon technologies that are programs, codes or commands embedded in files that alert defenders' systems when a file marked with a beacon is modified or accessed outside the company's system.

Paul Rosenzweig offers a useful ACD typology based on the effects of its application.[29] Less aggressive ACD measures, categorised as 'internal self-defence', may include:
- creating attractive honeypots with hidden payloads to track attackers within the defender's system or observe attempts at data removal;
- utilising threat intelligence to screen or block incoming traffic associated with threat indicators, such as blocking suspicious IP addresses;
- restricting network access during certain internal manipulations of data to prevent exfiltration;
- employing canary-trap markings on data for easy identification of illegal activity upon its reuse.

More aggressive active defence types extend beyond the defender's network boundaries and impact the attacker's or intermediate locations. These actions involve, for example:
- utilising described payloads to pinpoint intermediate or originating server sites;
- progressing beyond identification to take action against these sites, halting data exfiltration or collection;
- employing 'armed' payloads, such as zero-day exploits, which inflict actual harm either on the adversary's computer control or potentially within the systems of the data's ultimate user, who may or may not be aware of its origin.

The most aggressive methods range from intelligence-gathering and collecting evidence or information about the attacker (for example, capturing their image through their webcam), to 'hack-backs' (also termed 'back hacking', 'retaliatory hacking' or 'offensive countermeasures') – which involve infiltrating the attacker's network to reclaim

[28] "Active Defense Strategy for Cyber," *MITRE*, 1 July 2012, at https://www.mitre.org/news-insights/publication/active-defense-strategy-cyber, 10 January 2024.

[29] P. Rosenzweig, "International Law...".

stolen data, alter it or even delete it. As Robert Dewar explains: *Hack-back is not a specific tool but a technique.*[30] It involves analysing an intrusion to identify the perpetrators and technology sources responsible for a cyberattack and hacking them in return to neutralise their efforts. The attackers' own tools are used against them; however, this crucially takes place in their systems and networks. Perhaps the most contentious approach is the potential for hack-backs to inflict damage on the attacker's networks or computers, aiming to prevent further losses or retaliate against the attacker.[31]

This categorisation of these measures is a requisite simplification. The problem of assigning cyber defence to a specific category is complicated by the fact that the same tactic can be applied in all three categories. For instance, honeypots are typically assigned to the passive defence category. If a honeypot infects intruders with a tracking beacon, enabling cyber defenders to determine the intruder's location, it would be categorised as active-passive. Additionally, if the same honeypot attached a virus capable of deleting all the data on the intruder's home system, it would qualify as active defence.[32] Wyatt Hoffman and Ariel E. Levite expand Rosenzweig's typology by incorporating other factors, including the profile of the targets (unwitting participants in an attack, innocent third parties or adversary networks), the temporal nature of the effects (temporary, extended or permanent), the scope (localised or broader) of an attack and the degree to which the ACD measures are automatic and autonomous. Naturally, these dimensions do not always align, but it is feasible to position common measures on a spectrum based on the level of their aggressiveness.[33]

THE CURRENT STATE OF AFFAIRS

When the U.S. government is capable of striking back in cyberspace and extending retaliation measures against assailants beyond the confines of its own internal computer networks,[34] private companies are restricted from using such measures – owing to the potential violation of the stipulations outlined in the Computer Fraud and Abuse Act (CFAA).[35] Despite uncertainties surrounding the explicit prohibition of active cyber defence measures by the CFAA,[36] it is evident that (according to it): *a victim*

30 R.S. Dewar, *CSS Cyber Defence...*, p. 8.

31 W. Hoffman, A.E. Levite, *Private Sector Cyber Defense...*

32 Ibid.

33 Ibid., p. 9.

34 J.N. Miller, R.J. Butler *National Cyber Defense Center: A Key Next Step toward a Whole-of-Nation Approach to Cybersecurity*, Baltimore 2021, at https://www.jhuapl.edu/sites/default/files/2022-12/NationalCyberDefenseCenter.pdf, 12 December 2023.

35 "9-48.000 – Computer Fraud and Abuse Act," *U.S. Department of Justice*, at https://www.justice.gov/jm/jm-9-48000-computer-fraud, 12 January 2024.

36 A. Berengaut, T. Austin, "Litigation Options for Post-Cyberattack 'Active Defense,'" *LAW360*, 29 October 2018, at https://www.cov.com/-/media/files/corporate/publications/2018/10/litigation_options_for_postcyberattack-_active_defense.pdf, 20 December 2023.

organisation should refrain from independently retaliating to a cyber incident by accessing, altering, or harming a computer it neither owns nor operates, even if the computer seems to have been implicated in an attack or intrusion.[37] The stance of the Justice Department's Computer Crime and Intellectual Property Section (CCIPS)[38] on this matter has remained unchanged for many years: *Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as 'hacking back' into the attacker's computer—even if such measures could, in theory, be characterised as 'defensive'. Doing so may be illegal, regardless of the motive*.[39]

Nevertheless, the technological and geopolitical landscape has undergone significant changes since the enactment of the CFAA in 1986 (adopted at a time when fewer than 20% of Americans owned a computer);[40] laws and regulations have been slow to adapt to these transformations.[41] This has created a situation in which the existing legal framework is not flexible enough to address contemporary challenges. For example, the CFAA makes it illegal to access or intercept data on a system that you do not own. However, the law does not clearly define what constitutes unauthorised access. This ambiguity has led to numerous legal disputes, as businesses and individuals attempt to determine what is permissible under the law. The Wiretap Act, the Electronic Communications Privacy Act (ECPA) and the federal prohibition on Pen Register Track and Trace (PRTT) devices also restrict access to data in certain cases. However, these laws are outdated and do not cover the full range of data that is now available online.[42]

The regulatory challenges surrounding the cyber activities of the private service sector underscore a fundamental conflict between states' aspirations to control cyber means and the private sector's imperative to safeguard itself by leveraging its skills, capabilities and strong motivations.[43] It is notable that cybersecurity is predominantly a commodity traded within the private market, necessitating its independent management by private, governmental and corporate end users. As the internet evolved, the private cybersecurity market expanded to cover various facets, ranging from basic

[37] "9-48.000 – Computer Fraud...".

[38] S. Baker, "RATs and Poison II – The Legal Case for Counterhacking," *The Volokh Conspiracy*, 14 October 2012, at https://volokh.com/2012/10/14/rats-and-poison-ii-the-legal-case-for-counterhacking/, 10 January 2024.

[39] Office of Legal Education Executive Office for United States Attorneys, *Prosecuting Computer Crimes*, Washington, D.C. 2010, at https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ccmanual_0.pdf, 1 January 2024.

[40] N. Winstead, "Hack-Back: Toward a Legal Framework for Cyber Self-Defense," *American University*, 26 June 2020, at https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm, 6 March 2025.

[41] D. Broeders, "Private Active Cyber Defense...".

[42] Ch. Cook, "Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook," *Stanford Law & Policy Review*, vol. 29, no. 2 (2018), pp. 205-236, after: D. Broeders, "Private Active Cyber Defense...".

[43] W. Hoffman, A.E. Levite, *Private Sector Cyber Defence...*

consumer protection to high-level national security measures.[44] Similarly, the relationship of states with the internet has shifted from a stance of inattention to one of significant security concern thanks to the internet's pivotal role in state economies and societies. Consequently, security concerns have escalated both quantitatively and qualitatively, giving rise to sophisticated cybercrime, digital espionage and state-led cyber operations.[45]

The official U.S. government stance reflects and aligns with the current legal situation. In the 'best practices' document drafted by the Cybersecurity Unit, the U.S. Department of Justice actively discourages the implementation of exploitative active defence measures: *a victim organisation should not unilaterally respond to a cyber incident by accessing, modifying, or damaging a computer it does not own or operate, even if the computer appears to have been involved in an attack or intrusion. Regardless of the victim's motive, doing so may violate federal law and possibly also the laws of many states and foreign countries, if the accessed computer is located abroad.*[46] Similarly, in a speech delivered in 2015, Assistant Attorney General Leslie R. Caldwell unequivocally denounced the use of strike-back techniques by firms and other private actors in any manner.[47] The concerns regarding ACD primarily centre around doubts regarding its effectiveness and the risk of escalation (see Chapter 3). Additionally, Jeanette Manfra, former Assistant Director for Cybersecurity for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), stated that: *we see some gaps between what an entity might consider adequate security for themselves or their sector and what is in the public's interest.*[48] Her emphasis has often centred on fostering collaboration and adopting proactive defence strategies rather than engaging in offensive cyber operations. The current Director of CISA, Jen Easterly, also focuses on minimising gaps in governmental inter-agency coordination and with the private sector, rather than arming the private sector with ACD capabilities.[49]

On the other hand, there are compelling grounds for suggesting that ACD (excluding hack-backs), if conducted with professionalism and responsibility, could serve

---

[44] Ibid.

[45] D. Broeders, "Private Active Cyber Defense...".

[46] United States Department of Justice, *Best Practices for Victim Response and Reporting of Cyber Incidents*, Washington, D.C. 2018, p. 23, at https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf, 10 January 2024.

[47] L. Kello, *The Virtual Weapon and International Order*, New Haven 2017, p. 236.

[48] "Press Briefing on the Attribution of the WannaCry Malware Attack to North," *White House*, 19 December 2017, at https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/, 20 February 2024.

[49] M.P. Fischerkeller, E.O. Goldman, R.J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, Oxford 2022; S. Ikeda, "CISA Expands Public-Private Partnerships for Cyber Defense, Calls on Silicon Valley to Bolster Cloud Security & Fight Ransomware Attacks," *CPO Magazine*, 11 August 2021, at https://www.cpomagazine.com/cyber-security/cisa-expands-public-private-partnerships-for-cyber-defense-calls-on-silicon-valley-to-bolster-cloud-security-fight-ransomware-attacks/, 11 February 2024.

as a valuable supplement to the arsenal available to private sector entities for safeguarding their critical assets and mitigating the impact of attacks.[50] Therefore, despite the emergence of critical voices characterising ACD as an untenable cybersecurity policy, recent political discourse demonstrates a diminishing presence of such fervent opposition. During his keynote address on cyber threats and next-generation cyber operations at the annual Cybersecurity Technology Summit, Admiral Michael Rogers, Director of the National Security Agency (NSA), voiced concerns regarding the participation of the corporate sector in ACD. However, he acknowledged that such collaboration has occurred in the past – when nation states lacked the capacity to address certain challenges on their own.[51] Some other government officials have subtly referenced the concept and practice of ACD in more neutral and supportive tones.[52] For example, during a panel discussion at the Aspen Security Forum in 2011, General Michael Hayden, former Director of both the NSA and the CIA, proposed the following: *Let me give you a provocative idea: what do you think about a digital Blackwater?*[53] He suggested that certain defence activities, even in physical spaces, have been privatised and that now there is a new realm in which the scope of government actions – or limitations on government actions – is not clearly defined.[54]

Despite radical and moderate voices of criticism of private ACD as a policy choice, some policymakers at both the federal and state levels in the United States, as well as internationally, are actively lobbying to grant companies more freedom to engage in such activities. The policy has demonstrated remarkable resilience, even being incorporated into the 2016 Republican National Committee (RNC) Platform.[55] The biggest supporter of the concept of ACD and introducer of the Active Cyber Defense Certainty Act (the so-called 'Graves bill'), Rep. Tom Graves, believes that hacking back can be a powerful tool to deter attackers and recover stolen data; however, he asserts that it must be done responsibly and within the law.[56] Also, Stewart Baker, former Assistant Secretary of the Department of Homeland Security, has actively lobbied for hacking back.[57] Therefore,

50 W. Hoffman, A.E. Levite, *Private Sector Cyber Defence...*

51 "NSA Director on Cybersecurity Threats," *C-SPAN*, 2 April 2015, at https://www.c-span.org/video/?325152-1/nsa-director-cybersecurity-threats, 20 February 2024.

52 D. Broeders, "Private Active Cyber Defense...".

53 A. Nusca, "Hayden: 'Digital Blackwater' May Be Necessary for Private Sector to Fight Cyber Threats," *ZDNET*, 31 July 2011, at https://www.zdnet.com/article/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/, 20 February 2024; after: D. Broeders, "Private Active Cyber Defense...", p. 6.

54 Ibid.

55 S. Shackelford, D. Charoen, T. Waite, N. Zhang, "Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking," *University of Pennsylvania Journal of International Law*, vol. 41, no. 2 (2018), p. 381.

56 B.A. Boateng, "Hack Back," *Medium*, 3 July 2023, at https://medium.com/@benjaminaffengboateng/hack-back-5bada6357d5, 12 February 2024.

57 S. Baker, "The Case for Limited Hackback Rights," *The Washington Post*, 22 July 2016, at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/22/the-case-for-limited-hack

there are increasing pressures to loosen the restrictions that currently ban or limit certain forms of ACD (in bolder proposals, not excluding hack-back).

In May 2013, the Commission on the Theft of American Intellectual Property suggested potential alterations to the relevant laws, proposing that private sector companies be granted the authority to retaliate against attackers through hacking.[58] However, it refrained from officially endorsing this contentious stance. As stated in the report, *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.*[59] Indeed, several companies are presently investigating methods for tracking down attackers who may be violating the Computer Fraud and Abuse Act (CFAA). An analysis of incident reports from various cybersecurity firms reveals that some security researchers have, for example, accessed command-and-control servers to gather intelligence about attackers. Bruce Schneier, a world- renowned computer security professional, acknowledges this practice, comparing it to international bribery: *It's illegal and you can't do it, but it's happening.*[60] As a result, new legislative proposals aim to legalise these limited measures.

With pressure increasing for the granting of private sector offensive capabilities, the U.S. Congress was urged to introduce legislation aimed at addressing this issue. Two notable bills emerged, one in the Senate in 2021 (S2292, Study on Cyber-Attack Response Options Act[61]) and one in the House in 2019 (H.R.3270, Active Cyber Defense Certainty Act[62]), both exploring the potential for private sector involvement in the cyber domain. Presently, neither bill has gained significant momentum. However, given the heightened role of hacktivists targeting private sector entities (e.g., during the Russia-Ukraine war), the need for action is evident.[63]

The Active Cyber Defense Certainty Act, colloquially referred to as the 'Hack-Back bill', was first proposed in 2017 and reintroduced in 2019. It emerged as a notably audacious legislative initiative, igniting impassioned discussions among experts about the critical issues and challenges linked to broadening the authority of private companies

back-rights/, 10 January 2024; S. Shackelford, D. Charoen, T. Waite, N. Zhang, "Rethinking Active Defense...".

58 I. Emilio, "Private Sector Hack-Backs Are a Recipe for Disaster," *Strike Source*, 24 November 2023, at https://strikesource.com/2023/11/24/private-sector-hack-backs-are-a-recipe-for-disaster/, 15 January 2024.

59 The National Bureau of Asian Research, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*, May 2013, at https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf, 11 January 2024.

60 R. Lemos, "Why the Hack-Back Is Still the Worst Idea in Cybersecurity," *TechBeacon*, at https://techbeacon.com/security/why-hack-back-still-worst-idea-cybersecurity, 11 January 2024.

61 S. Daines, "S.2292 – Study on Cyber-Attack Response Options Act," *Congress*, 24 June 2021, at https://www.congress.gov/bill/117th-congress/senate-bill/2292/text?s=1&r=14, 20 December 2023.

62 T. Graves, "H.R.3270 – Active Cyber Defense Certainty Act," *Congress*, 13 June 2019, at https://www.congress.gov/bill/116th-congress/house-bill/3270/actions, 20 December 2023.

63 I. Emilio, "Private Sector Hack-Backs...".

to employ novel forms of ACD. While this legislation failed to pass, its provisions had the potential to be incorporated into another bill and subsequently become law. Rep. Tom Graves, the primary sponsor of the bill, explained that: *At a time when the federal government is struggling to defend its own networks, it's unsurprising that they don't have the capability to respond effectively to millions of cyberattacks targeting individuals and businesses* and *When the lack of response is combined with the changing economic forces making hacking more lucrative for criminals, the trend will only get worse unless changes are made.*[64]

This bipartisan legislative proposal aims to introduce two novel exemptions to the CFAA, affirming that the existing legislation does not prohibit retaliatory hacking. Firstly, the ACDC aimed to modify the CFAA by explicitly permitting specific attribution technologies to be utilised for identifying cyber intruders. Secondly, and subject to specific conditions, the proposal sought to establish immunity from CFAA prosecution for active cyber defence tactics, encompassing defensive actions such as unauthorised access to the attacker's computer to gather crucial attribution data, disrupt particular ongoing authorised activities or surveil the attacker's conduct in order to develop effective 'cyber defence techniques'.[65]

According to the ACDC, a 'defender' is defined as *a person or an entity that is a victim of a persistent unauthorised intrusion of the individual entity's computer*, whereas an 'active cyber defence measure' is described as *any measure undertaken by, or at the direction of, a defender; and consisting of accessing without authorisation the computer of the attacker to the defender's own network to gather information.*[66] The legislation specifies that the newly granted powers are reserved for 'qualified defenders' who possess 'a high degree of confidence in attribution' regarding the identity of their attackers. Prior to engaging in retaliatory actions, they are required to notify the FBI and solicit guidance while also making concerted efforts to prevent harm to third-party systems and to prevent the escalation of conflicts.

While these safeguards may seem reasonable at first glance, the ACDC Act is fundamentally flawed for several reasons. The law is intended to guarantee that retaliatory actions can be conducted under specific conditions, reducing harm to victims and deterring certain network intrusions. However, it may simultaneously trigger numerous unintended consequences for both the assailant and the victim, as well as uninvolved, innocent parties. Furthermore, retaliatory actions undertaken without the involvement of law enforcement agencies may evoke other, less favourable associations with vigilantism, wherein punishment is meted out by unauthorised individuals or institutions. In democratic states, vigilantism is, of course, illegal, and the prosecution of crimes is entrusted to specialised state authorities to ensure impartiality and detachment from

[64] T. Graves, "Let's Make Hackers Think Twice," *The Hill*, 25 October 2017, at https://thehill.com/opinion/cybersecurity/357004-lets-make-hackers-think-twice/, 20 January 2024.

[65] P.G. Berris, "Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes," *Congressional Research Service*, 16 May 2023, p. 45, at https://crsreports.congress.gov/product/pdf/R/R47557, 11 January 2024.

[66] T. Graves, "H.R.3270 – Active Cyber Defense...".

emotional impulses. Therefore, regardless of the potentially positive effects of the ACDC Act, the threats it would entail should not be underestimated.

Along with the concerns shared by experts related to private ACD, such as the problem of attribution, risk of escalation and insufficient corporate readiness (see Chapter 3), the challenges associated with the implementation of the ACDC Act include the problem of supervision of ACDM (Active Cyber Defense Measures) and definitional ambiguity.

When it comes to supervision, the FBI Cyber Investigative Joint Task Force should only be notified of the intention to conduct a cyberattack after obtaining a high degree of certainty about the source of the attack and receiving confirmation that the notification has been sent. The notification must include the type of cyber intrusion suffered by the individual or entity, the intended target of the active cyber defence measure, the steps the defender plans to take to preserve evidence of the attacker's cybercrime, the steps they plan to take to prevent damage to proxy computers that are not owned by the attacker and other information required by the FBI to assist in oversight. While informing the FBI about the use of ACDM is mandatory, disclosing the exact techniques to be used is voluntary. It can be assumed that the attack victim will not wait for formal permission from the FBI and, in extreme cases, may even go beyond taking the actions they have declared.[67] Taking everything into account, it seems likely that the assurances of accountability will not be implemented as originally intended. Furthermore, the ACDC project provides scant information regarding oversight measures beyond the voluntary review of actions by the FBI. The National Cyber Investigative Joint Task Force will have to develop its own internal supervision procedures and guidelines for companies. It remains unclear how thoroughly the FBI will supervise the active cyber defence programs implemented by companies, and it is possible that these will not always receive sufficient guidance to operate within the boundaries of the law. The quality of ACDC implementation depends not only on the interested companies themselves, but also on the internal procedures and regulations of the FBI.

Based as it is on definitional ambiguity, the project also encompasses a significant degree of linguistic uncertainty, which could ultimately hinder the implementation of the law.[68] For instance, imprecise terminology such as 'persistent unauthorised intrusion' can lead to confusion. This term was likely introduced to prevent companies from invoking ACDC when they merely experience inconvenience on their computer network. It refers to the duration of a specific intrusion or series of intrusions, but ultimately it is unclear what length of time is sufficient to deem them persistent. Because the term leaves room for interpretation, it raises the question of whether the victim can actually benefit from the provisions of the law. It is also worth noting that even short-term intrusions can have serious consequences, which the legislator did not take into account. The law defines an 'attacker' as *a person or an entity that is the source of the persistent unauthorised intrusion into the victim's computer.* However, this lacks

[67] Ch. Cook, "Cross-Border Data Access...".

[68] Ibid., p. 216.

clarification on what constitutes the 'attacker's computer.' As mentioned earlier, an attack can pass through a chain of infected computers, so an intrusion may involve not just one but many of them, making it difficult to determine the actual source of the attack. The new, updated version of the law attempts to address these ambiguities by introducing the definition of an 'intermediary computer', which means *a person or entity's computer that is not under the ownership or primary control of the attacker but has been used to launch or obscure the origin of the persistent cyber-attack.* Still, in situations where intermediary computers are under the control of the attacking party, attributing the origin of the attack will be challenging. Ultimately, companies intending to target intermediary computers may struggle to determine whether such actions would violate the law. The law provides exceptions that hold entities accountable for activities falling outside the scope of ACDC. These include actions that intentionally exceed the level of activity required to conduct reconnaissance on an intermediary computer in order to attribute the source of a persistent cyberattack, or actions that deliberately cause intrusion or remote access to an intermediary computer. While such provisions have clear justifications, they also leave room for interpretation, as it remains uncertain whether gaining access to an intermediary computer solely for reconnaissance purposes and attributing the source of the attack will be regarded as intentionally gaining remote access to that computer. Among other unspecified situations in which a company may be liable for counterattacks are those where, among other things, the targeted company *creates a threat to the public health or safety* or when its action *intentionally results in the persistent disruption to a person or entities internet connectivity.* The draft law does not specify what constitutes a threat to health or public safety or what constitutes a persistent disruption.

SECURITY RISKS OF LEGALISING PRIVATE ACD

It is possible that an excessively permissive environment enabling private sector engagement in ACD could result in ill-equipped defenders conducting ACD, potentially causing systemic destabilisation effects. The utilisation of cyber arms by the private sector presents at least three risks: (1) improper attribution; (2) unpreparedness of private firms for the application of ACD; and (3) inadvertent or escalating international conflict. The latter directly implicates state interests and represents a potentially severe threat.

The initial concern pertains to the potential misattribution of a cyberattack. Active cyber defence encompasses three key phases: (1) detection, which involves identifying and recognising an ongoing attack; (2) traceback, which entails determining the source of the attack, akin to employing a traceroute tool; and (3) counterstrike, which involves taking action to mitigate or neutralise the attack's impact.[69] However, attackers often employ tactics like IP spoofing to mask their true location, for example, by using proxy

[69] S. McGee, R.V. Sabett, A. Shah, "Adequate Attribution...", pp. 12-13.

servers and chains of infected computers belonging to innocent third parties, which hinders effective traceback. Additionally, it is difficult to be certain that the computer that appears to be the source of the attack has not itself been compromised.

As shown by a recent analysis from the University of Surrey and Hewlett Packard, over 200 cybersecurity incidents related to state-sponsored activities have occurred since 2009; half of them involved low-budget, simple tools readily available for purchase on the dark web, while an additional 20% comprised more sophisticated custom--made weaponry. However, another 30% had uncertain or unattributable origins. If the latter types of attack are conducted skilfully, attackers will not, in most cases, provide investigators with sufficient evidence to establish the source of the offensive activity. Therefore, although advances in tracing cyberattacks and sophisticated digital forensics have empowered intelligence agencies and private-sector cybersecurity firms to determine with reasonable certainty the perpetrators behind the majority of attacks,[70] attribution still arises as the most significant issue around active defence .[71] It remains a slow, multi-stage process that rarely provides certainty about the origin of the attack. Despite the many factors that can enable attribution, including technical, political and intelligence indicators, as well as the common practices and craftsmanship employed by various experts in the field of cyber forensics, uncertainty about the origin of an attack can be minimised, but the high level of certainty desired is rarely achieved. Furthermore, as private entities and government agencies persistently develop innovative traceback methods, the specifics of these advancements remain confidential for obvious security reasons.[72]

For the above reasons, the attribution problem poses a significant challenge, especially when considering aggressive extraterritorial responses like hack-backs. In practice, even establishing the likelihood of the origin of attacks requires specialised resources, such as a qualified team and appropriate means. Therefore, it is crucial to reiterate its importance in the context of ADC strategies, particularly when such strategies might involve kinetic responses. While pinpointing the origins of attacks is not impossible, the anonymity offered by the digital space makes it highly complex and resource--intensive.[73] Accordingly, employing hack-backs as a response necessitates a high degree of confidence in the accuracy of the identification of a source. In other words, the defending party must be certain, beyond reasonable doubt, that the culprit identified is, in fact, the true one, considering the potential legal repercussions discussed earlier. This need for certainty is significantly amplified when nation-states are involved, as they reserve the right to retaliate with conventional weaponry in response to cyberattacks.

---

70 S. Gordon, E. Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs*, vol. 101, no. 1 (2022), p. 18.

71 P. Lin, "Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies," *A Policy Paper on Cybersecurity*, 26 September 2016, pp. 1-34; D. Alperovitch, "The Case for Cyber-Realism: Geopolitical Problems Don't Have Technical Solutions," *Foreign Affairs*, 14 December 2021, at https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism, 17 December 2023.

72 Ibid.

73 R.S. Dewar, "The 'Triptych of Cyber Security'...", p. 11.

The consequence of incorrectly attributing the source of an attack may be attacking the wrong systems or causing harm to uninvolved entities. Therefore, meeting the condition for the application of appropriate Active Cyber Defense Measures (ACDM), which is obtaining a high degree of certainty about the source of the attack, is practically unrealistic. To reduce the problems associated with attributing a cyber incident to its perpetrators, ACDC would legalise the use of beacon technology (i.e., programs, scripts or commands embedded in files that signal to defence systems when a file marked with a beacon is modified or accessed outside the company's system). This would allow the tracking of the path and location of the stolen file, providing potentially stronger but still uncertain evidence of attribution.

Secondly, underfunded companies usually do not have well-defined strategies or methods of operation in cyberspace. The ACDC bill does not specify exactly what makes a company or individual a 'qualified defender'. Therefore, it can be assumed that such actions may be taken by both experienced IT sector giants and small, unprepared companies.[74] Since most companies struggle to adhere to basic cyber hygiene principles, such as conducting awareness training among employees on security, regularly backing up data and regularly patching security vulnerabilities, it is difficult to expect them to have the skills and tools to carry out precise and controlled counter-attacks. As a result, it is impossible to predict their ultimate consequences. Accordingly, Sean Weppner, a former DoD officer, contends that hacking back should be exclusively entrusted to governments. He asserts that: *Only a select few possess the requisite experience and expertise to execute this action with the necessary level of sophistication and restraint.*[75] This viewpoint is shared by Alex Bolling, former Chief of Operations at the CIA's Information Operations Center, who believes that USCYBERCOM is the best-equipped agency to address threats to U.S. national interests and critical infrastructure across the energy, finance and broader commercial sectors. Allowing companies to engage in hacking back would effectively empower a form of cyber vigilantism, potentially leading to significant and perilous outcomes. Among these is the risk that companies operating in foreign networks could inadvertently disrupt ongoing U.S. intelligence or military operations.[76]

Establishing a market for private ACD might potentially resolve the issue of insufficient readiness. However, it will inevitably raise new questions that echo the ongoing debates regarding the privatisation of security as a whole and the delivery of public-private cybersecurity in particular.[77] Therefore, public-private governance solutions for security problems must navigate a complex interplay between three key considerations:

---

74 M. Giles, "Five Reasons 'Hacking Back' Is a Recipe for Cybersecurity Chaos," *MIT Technology Review*, 21 June 2019, at https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/, 21 February 2024.

75 Ibid.

76 R. Duffy, "Private Sector Warms to U.S. Cyber Command Carrying out 'Hack Backs,'" *CyberScoop*, 19 June 2018, at https://cyberscoop.com/cyber-command-hack-back/, 21 February 2024.

77 D. Broeders, "Private Active Cyber Defense...", p. 3.

the allocation of capacity and responsibility, the political legitimacy of such solutions and the mitigation of their potential negative external effects.[78]

Despite critical voices being raised, it cannot be denied that the ACDC Act fits into the American way of thinking about ensuring security for citizens and intensifies the contemporary trend of the fusion of state and non-state actors. Where the state cannot guarantee security, powers should be granted to citizens or private entities. However, equipping private entities with cyberweapons further blurs these lines, raising concerns about accountability and control. Moreover, legalising ACD raises legitimate concerns primarily due to vague provisions, potential side-effects and possible unintended international consequences. The risk of escalation through misattribution of the source of an attack may prove to be too significant an obstacle for the legislative proposal to be accepted in its current form. Despite the obvious need to grant private companies additional powers to protect their networks, the most important question concerns the price to be paid for these additional capabilities. Admiral Michael Rogers, head of the NSA, when asked whether active defence should be legal, gave this response: *While there is certainly historic precedent for this—nation states have often gone to the private sector when we lacked government capacity or capability... my concern is, [I would] be leery of putting more gunfighters out on the street in the wild west.*[79] Indeed, sometimes politicians, when trying to solve a problem, only exacerbate the situation. Politicians advocating for the introduction of ACDC fail to understand that corporate gunslingers may lack the necessary resources and skills and may not even know what to aim for. In light of all these doubts, it is not surprising that ACDC has close to zero chance of being implemented.

Thirdly, enabling private companies to engage in active cyber defence introduces significant practical, legal and international appearance risks with potential international security implications. From a practical standpoint, private ACD initiatives carry the risk of escalation beyond legal boundaries. Even activities operating beneath the threshold of aggression may be perceived as disruptive or offensive, leading to potential conflict escalation between states or the exploitation of situations for the purposes of escalation. Furthermore, the primary worry revolves around the possibility of an international crisis stemming from an increasing cycle of cyberattacks and retaliatory measures between companies based in two different states or a company intentionally or unintentionally targeting the intelligence or military of another state. The situation would be even more complicated were an attack to be conducted by a state-sponsored actor. For instance, if North Korea were to infiltrate the information systems of a prominent American IT firm, the adverse international repercussions might outweigh any perceived benefits of the attack. Therefore, James Lewis at the Center for Strategic and International Studies calls the notion *a remarkably bad idea that would harm the national interest* and that *encouraging*

[78] Ibid.

[79] G. Santistevan, "The Case against Hacking Back," *Georgetown Security Studies Review*, 11 December 2017, at https://georgetownsecuritystudiesreview.org/2017/12/11/the-case-against-hacking-back/, 15 January 2024.

corporations to compete with the Russian mafia or Chinese military hackers to see 'who can go further in violating the law' is not a contest American companies can win.[80]

Opponents of ACD contend that if a company retaliates against a hacker, the initiator is unlikely to retreat.[81] This risk is heightened if the attacking hacker originates from another nation or is backed by a foreign government; often, cyber threats stem not from private entities but from state-sponsored hackers. While it is conceivable for a company to perceive itself as being in conflict with a hacker, the situation grows graver if the target of a hack-back is government-supported. Patrick Lin highlights the point that companies (or individuals) lack the ability to accurately predict a cyber adversary's response to a hack-back.[82] Additionally, it is challenging to prevent the target of a hack-back from misinterpreting it as state-sponsored. For this reason, Lin portrays hack-back as *the initial salvos of a cyberwar, which could escalate into a physical or kinetic conflict.*[83]

Moreover, the enactment of ACDC legislation could set a precedent, prompting other nations to relax their anti-hacking regulations, and, as Sandra Joyce of FireEye put it: *That would create an even higher risk of a cyber catastrophe.*[84] It is also worth noting that by shifting some state powers to private companies, there may be a concern about the public perception of such actions, understood as the state's weakness in maintaining a monopoly on the use of force. There is also a risk that states will gradually reduce their oversight of the activities undertaken by companies in cyberspace, even if they exceed the bounds of the law. The consequence of such a development may be the loss of state control over ACD.

From a legal perspective, various considerations emerge, with two primary aspects standing out. Firstly, there is uncertainty regarding whether the activities conducted by private entities could be deemed aggressive under international law and consequently invite retaliatory measures. International law lacks substantial clarity regarding the treatment and protocols concerning private ACD.[85] While active cyber defence typically operates in the grey zone, below the level of hack-backs, the possibility of political framing by aggrieved adversaries cannot be discounted. Secondly, as noted by Josephine Wolff, legalising such activities under U.S. jurisdiction does not guarantee compliance with the laws of other nations.[86] The legislation advises practitioners of active defence

[80] M. Fisher, "Should the U.S. Allow Companies to 'Hack Back' against Foreign Cyber Spies?," *The Washington Post*, 23 May 2013, at https://www.washingtonpost.com/news/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/, 11 February 2024, after: Ch. Cook, "Cross-Border Data Access...", p. 220.

[81] K. Gerke, "Canadian Hack-Back?: A Consideration of the Canadian Legal Framework for Private--Sector Active Cyber Defence," *Alberta Law Review*, vol. 59, no. 1 (2021), p. 197.

[82] P. Lin, "Ethics of Hacking Back...".

[83] Ibid., p. 15.

[84] M. Giles, "Five Reasons...".

[85] W. Hoffman, A.E. Levite, *Private Sector Cyber Defense...*, p. 17.

[86] J. Wolff, "Attack of the Hack Back: The Worst Idea in Cybersecurity Is Back Again," *Slate*, 17 October 2017, at https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html, 20 February 2024.

to exercise caution to avoid violating foreign laws, necessitating private firms to assess the risk of violating both U.S. and foreign laws. Given that the ACDC bill constitutes U.S. legislation, the question arises as to whether U.S. companies engaging with servers in foreign jurisdictions might inadvertently contravene the laws of those countries. Moreover, national legislation, including that of the United States, frequently demonstrates ambiguity or a lack of clarity regarding the permissibility of various forms of authorised countermeasures, except in extreme circumstances. It is probable that ACD actions, even those causing harm or accessing computers in other countries, could violate the domestic laws of the affected country, thereby exposing the defender to legal repercussions within that jurisdiction.[87]

Finally, James Lewis argues that permitting individuals or companies to engage in hack-back would constitute a violation of international norms against such activity, which the United States has long advocated for.[88] Even actions that fall short of hack-back, such as unauthorised access to foreign networks, could undermine the U.S.' credibility in international norm-building efforts. Lewis emphasises that by enacting the ACDC legislation without first establishing international consensus, the U.S. would implicitly contradict its own efforts to outlaw unauthorised hacking. It would reveal the insincerity of American cybersecurity policy. In the actions of the American government, some may perceive hypocrisy: on the one hand, it calls for the establishment of common security standards, but the practical actions of the Americans contradict this.

CONCLUSIONS

With the escalating frequency and severity of cybercrime, there is a growing debate about whether companies should be empowered to engage in 'digital vigilantism', actively taking measures to prevent or address cyber incidents. The notion of legalisation holds appeal from both corporate and political perspectives, especially during times of mounting frustration, as it suggests that action can be taken whenever industry and politicians demand it. However, two questions follow: would such legalisation be effective, and at what cost? Given this perspective, a strong case for the legalisation of Active Cyber Defense in some forms exists.

As stated in the article, many critics of ACD have framed the debate in binary terms: it is seen as either legal or illegal and as either enhancing cybersecurity or posing a threat to the international order. Moving forward, it is essential to acknowledge the various forms that ACD might assume. Looking forward, the United States needs to engage in a dialogue regarding the possibilities of ACD both domestically and internationally, focusing on determining the appropriate distribution of responsibility for cybersecurity between the government and the private sector. While the legislative

[87] W. Hoffman, A.E. Levite, *Private Sector Cyber Defense...*, p. 17.

[88] M. Fisher, "Should the U.S. Allow Companies...".

proposal for the Active Cyber Defense Certainty Act may serve as the initiation of this discourse, it by no means signifies its conclusion. It is essential to conduct further exploration in this matter, to determine how the U.S. government can aid the private sector in addressing its urgent need for improved cybersecurity, while avoiding the Jason Healey scenario, in which the internet *would no longer be merely the wild west, but a failed state like Somalia*.[89]

Moreover, the discussion surrounding private sector ACD extends beyond simply permitting companies to engage in specific technical actions. At its core, it revolves around delineating the roles and contributions of both the government and private sector in cybersecurity. Therefore, legislation at the domestic level, seeking to authorise private ACD, must be carefully aligned with the state's exclusive authority over the legitimate use of force. Such legislation should also address the potential ramifications of private companies disrupting state-to-state relations, exacerbating international tensions and encroaching on what states regard as their sovereign domain. The debate on reactive solutions for the private sector must navigate a delicate balance between the allocation of capacity and responsibility, the political legitimacy of such arrangements and the mitigation of their external impacts. Additionally, permitting a degree of involvement from the private sector in ACD does not automatically mean a permanent forfeiture of state authority. Nevertheless, efforts to ease or alter legal constraints regarding private sector ACD are not advisable until further data is gathered on the effectiveness of different ACD strategies and the feasibility of principled behaviour by private entities. Undoubtedly, the U.S. government must enhance its efficacy or risk a situation in which private solutions may prove difficult to control and could undermine governmental legitimacy. Similarly, this could be interpreted as a call for private firms to bolster the protection of their digital assets and, consequently, the overall cybersecurity of the private sector. Recognising that the more invasive parts of the ACD continuum, particularly hack-backs, are unlikely to find legal footing, experts and government officials may view the ACD debate as an opportunity to clarify the law and address the issue of underinvestment in cybersecurity within the private sector.

BIBLIOGRAPHY

"9-48.000 – Computer Fraud and Abuse Act," *U.S. Department of Justice*, at https://www.justice.gov/jm/jm-9-48000-computer-fraud.

"Active Defense Strategy for Cyber," *MITRE*, 1 July 2012, at https://www.mitre.org/news-insights/publication/active-defense-strategy-cyber.

[89] J. Healey, *A Nonstate Strategy for Saving Cyberspace*, Washington, D.C. 2017, p. 26, at https://www.atlanticcouncil.org/wp-content/uploads/2015/08/AC_StrategyPapers_No8_Saving_Cyberspace_WEB.pdf, 21 January 2024.

Alperovitch D., "The Case for Cyber-Realism: Geopolitical Problems Don't Have Technical Solutions," *Foreign Affairs*, 14 December 2021, at https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism.

Berengaut A., Austin T., "Litigation Options for Post-Cyberattack 'Active Defense,'" *LAW360*, 29 October 2018, at https://www.cov.com/-/media/files/corporate/publications/2018/10/litigation_options_for_postcyberattack-_active_defense.pdf.

Baker S., "The Case for Limited Hackback Rights," *The Washington Post*, 22 July 2016, at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/22/the-case-for-limited-hackback-rights/.

Baker S., "RATs and Poison II – The Legal Case for Counterhacking," *The Volokh Conspiracy*, 14 October 2012, at https://volokh.com/2012/10/14/rats-and-poison-ii-the-legal-case-for-counterhacking/.

Berinato S., "Active Defense and 'Hacking Back': A Primer," *Harvard Business Review*, 21 May 2018, at https://hbr.org/2018/05/active-defense-and-hacking-back-a-primer#:~:text=%E2%80%9CThis%20is%20a%20moment%20when.

Berris P.G., "Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes," *Congressional Research Service*, 16 May 2023, at https://crsreports.congress.gov/product/pdf/R/R47557.

Boateng B.A., "Hack Back," *Medium*, 3 July 2023, at https://medium.com/@benjaminaffengboateng/hack-back-5bada6357d5.

Broeders D., "Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?," *Journal of Cybersecurity*, vol. 7, no. 1 (2021), https://doi.org/10.1093/cybsec/tyab010.

Christen M., Gordjin B., Loi M., *The Ethics of Cybersecurity*, Cham 2020, https://doi.org/10.1007/978-3-030-29053-5.

Cook Ch., "Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook," *Stanford Law & Policy Review*, vol. 29, no. 2 (2018), pp. 205-236.

Daines S., "S.2292 – Study on Cyber-Attack Response Options Act," *Congress*, 24 June 2021, at https://www.congress.gov/bill/117th-congress/senate-bill/2292/text?s=1&r=14.

Dewar R.S., *CSS Cyber Defence Trend Analysis 1: Active Cyber Defense*, Zürich 2017, at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-03.pdf.

Dewar R.S., "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence," in *2014 6th International Conference on Cyber Conflict (ICCC)*, Tallinn 2014, pp. 7-21, https://doi.org/10.1109/CYCON.2014.6916392.

Duffy R., "Private Sector Warms to U.S. Cyber Command Carrying out 'Hack Backs,'" *CyberScoop*, 19 June 2018, at https://cyberscoop.com/cyber-command-hack-back/.

Dziwisz D., *USA and the International Cybersecurity*, Cracow 2010.

Emilio I., "Private Sector Hack-Backs Are a Recipe for Disaster," *Strike Source*, 24 November 2023, at https://strikesource.com/2023/11/24/private-sector-hack-backs-are-a-recipe-for-disaster/.

Fischerkeller M.P., Goldman E.O., Harknett R.J., *Cyber Persistence Theory: Redefining National Security in Cyberspace*, Oxford 2022, https://doi.org/10.1093/oso/9780197638255.001.0001.

Fisher M., "Should the U.S. Allow Companies to 'Hack Back' against Foreign Cyber Spies?," *The Washington Post*, 23 May 2013, at https://www.washingtonpost.com/news/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/.

Gerke K., "Canadian Hack-Back?: A Consideration of the Canadian Legal Framework for Private-Sector Active Cyber Defence," *Alberta Law Review*, vol. 59, no. 1 (2021), pp. 171-200, https://doi.org/10.29173/alr2668.

Giles M., "Five Reasons 'Hacking Back' Is a Recipe for Cybersecurity Chaos," *MIT Technology Review*, 21 June 2019, at https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/.

Gordon S., Rosenbach E., "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs*, vol. 101, no. 1 (2022), pp. 10-21.

Graves T., "H.R.3270 – Active Cyber Defense Certainty Act," *Congress*, 13 June 2019, at https://www.congress.gov/bill/116th-congress/house-bill/3270/actions.

Graves T., "Let's Make Hackers Think Twice," *The Hill*, 25 October 2017, at https://thehill.com/opinion/cybersecurity/357004-lets-make-hackers-think-twice/.

Healey J., *A Nonstate Strategy for Saving Cyberspace*, Washington, D.C. 2017, at https://www.atlanticcouncil.org/wp-content/uploads/2015/08/AC_StrategyPapers_No8_Saving_Cyberspace_WEB.pdf.

Healey J., *Shaping American Cyber Security Policy*, interview by D. Dziwisz, November 2013.

Hoffman W., Levite A.E., *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, Washington, D.C. 2017, at https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf.

Ikeda S., "CISA Expands Public-Private Partnerships for Cyber Defense, Calls on Silicon Valley to Bolster Cloud Security & Fight Ransomware Attacks," *CPO Magazine*, 11 August 2021, at https://www.cpomagazine.com/cyber-security/cisa-expands-public-private-partnerships-for-cyber-defense-calls-on-silicon-valley-to-bolster-cloud-security-fight-ransomware-attacks/.

"Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," *Center for Cyber and Homeland Security*, October 2016, at https://perma.cc/SAX8-4LW3.

Kello L., "Private-Sector Cyberweapons: Strategic and Other Consequences," *SSRN Electronic Journal*, 2016, pp. 1-24, https://doi.org/10.2139/ssrn.2836196.

Kello L., *The Virtual Weapon and International Order*, New Haven 2017, https://doi.org/10.2307/j.ctt1trkjd1.

Lachow I., "Active Cyber Defense: A Framework for Policymakers," *Center for a New American Security*, 22 February 2013, at https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers.

Lee R.M., *The Sliding Scale of Cyber Security: A SANS Analyst Whitepaper*, August 2015, at https://perma.cc/TU3K-XEFU.

Lemos R., "Why the Hack-Back Is Still the Worst Idea in Cybersecurity," *TechBeacon*, at https://techbeacon.com/security/why-hack-back-still-worst-idea-cybersecurity.

Lin P., "Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies," *A Policy Paper on Cybersecurity*, 26 September 2016, pp. 1-34, http://dx.doi.org/10.2139/ssrn.4682398.

Lynn III W.J. "Remarks on Cyber at the RSA Conference," *U.S. Department of Defence*, 15 February 2011, at http://www.defense.gov/speeches/speech.aspx?speechid=1535.

McGee S., Sabett R.V., Shah A., "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law*, vol. 8, no. 1 (2013), pp.1-47, at https://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3/.

Miller J.N., Butler R.J., *National Cyber Defense Center: A Key Next Step toward a Whole-of-Nation Approach to Cybersecurity*, Baltimore 2021, at https://www.jhuapl.edu/sites/default/files/2022-12/NationalCyberDefenseCenter.pdf.

Mueller III R.S. "Combating Threats in the Cyber World," *Federal Bureau of Investigation*, 1 March 2012, at https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

The National Bureau of Asian Research, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*, May 2013, at https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf.

"National Cybersecurity Strategy," *White House*, March 2023, at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

"NSA Director on Cybersecurity Threats," *C-SPAN*, 2 April 2015, at https://www.c-span.org/video/?325152-1/nsa-director-cybersecurity-threats.

Nusca A., "Hayden: 'Digital Blackwater' May Be Necessary for Private Sector to Fight Cyber Threats," *ZDNET*, 31 July 2011, at https://www.zdnet.com/article/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/.

Office of Legal Education Executive Office for United States Attorneys, *Prosecuting Computer Crimes*, Washington, D.C. 2010, at https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ccmanual_0.pdf.

Pattison J., "From Defence to Offence: The Ethics of Private Cybersecurity," *European Journal of International Security*, vol. 5, no. 2 (2020), pp. 233-254, https://doi.org/10.1017/eis.2020.6.

"Press Briefing on the Attribution of the WannaCry Malware Attack to North," *White House*, 19 December 2017, at https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

Rosenzweig P., "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law*, vol. 47, no. 2 (2013), pp. 1-13, https://doi.org/10.2139/ssrn.2270673.

Rudden J., "Business Risks Globally 2020," *Statista*, 22 August 2023, at https://www.statista.com/statistics/422171/leading-business-risks-globally/.

Santistevan G., "The Case against Hacking Back," *Georgetown Security Studies Review*, 11 December 2017, at https://georgetownsecuritystudiesreview.org/2017/12/11/the-case-against-hacking-back/.

Shackelford S., Charoen D., Waite T., Zhang N., "Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking," *University of Pennsylvania Journal of International Law*, vol. 41, no. 2 (2018), pp. 377-427, https://doi.org/10.2139/ssrn.3303407.

United States Department of Defense, *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02*, November 2010, at https://irp.fas.org/doddir/dod/jp1_02.pdf.

United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, at https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

United States Department of Justice, *Best Practices for Victim Response and Reporting of Cyber Incidents*, Washington, D.C. 2018, at https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

Van Dine A., "When Is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention," *Chicago Journal of International Law*, vol. 20, no. 2 (2020), pp. 530-564, at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1777&context=cjil.

Winstead N., "Hack-Back: Toward a Legal Framework for Cyber Self-Defense," *American University*, 26 June 2020, at https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm.

Wolff J., "Attack of the Hack Back: The Worst Idea in Cybersecurity Is Back Again," *Slate*, 17 October 2017, at https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html.

Dominika DZIWISZ – PhD, is an assistant professor in the Institute of Political Science and International Relations of the Jagiellonian University in Kraków, Poland. She holds master's degree both in International Relations as well as Marketing and Management. She received her PhD with distinctions from the Jagiellonian University in 2014. Her PhD research was focused on cybersecurity policy in the USA. This topic, together with critical infrastructure protection and the relationship between Big Data and human rights, to this day remains in the center of her research interests.