2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Permission to make digital or hard copies of this publication for internal use within NATO and for personal or educational use when for non-profit or non-commercial purposes is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission by NATO CCD COE.

The "Triptych of Cyber Security": A Classification of Active Cyber Defence

Robert S. Dewar
Department of Politics
University of Glasgow
Glasgow, United Kingdom
r.dewar.1@research.gla.ac.uk

Abstract: In the field of cyber security, ill-defined concepts and inconsistently applied terminology are further complicating an already complex issue[1]. This causes difficulties for policy-makers, strategists and academics. Using national cyber security strategies to support current literature, this paper undertakes three tasks with the goal of classifying and defining terms to begin the development of a lexicon of cyber security terminology. The first task is to offer for consideration a definition of "active cyber defence" (ACD). This definition is based upon a number of characteristics identified in current academic and policy literature. ACD is defined here as the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network. Once defined, ACD is contextualised alongside two further approaches to cyber defence and security. These are fortified and resilient cyber defence, predicated upon defensive perimeters and ensuring continuity of services respectively. This contextualisation is postulated in order to provide more clarity to non-active cyber defence measures than is offered by the commonly used term "passive cyber defence". Finally, it is shown that these three approaches to cyber defence and security are neither mutually exclusive nor applied independently of one another. Rather they operate in a complementary triptych of policy approaches to achieving cyber security.

Keywords: *active cyber defence; resilience; cyber security; definition; classification; triptych; lexicon*

1. INTRODUCTION – DEFINITION OF THE PROBLEM *IS* THE PROBLEM[2]

A fundamental difficulty facing the development of cyber defence measures, and the wider study of cyber security, is that of accurately defining the issues under scrutiny. Inconsistently applied terminology and concepts are further complicating an already complex issue. Raising

1 Dan Kruger, "Radically Simplifying Cybersecurity," 2012, 1, http://www.absio.com/sites/default/files/assets/Radically_Simplifying_Cybersecurity_V1.4_1.pdf.

2 Ibid.

this may appear pedantic, but the use of ill-defined and inconsistent terms creates difficulties for policy makers in developing strategies to address the risks inherent in an increasingly wired society[3]. In order to begin the process of developing a comprehensive, cohesive lexicon of cyber security terminology a definition of one key feature – active cyber defence – is proposed here. The definition offered is predicated upon proactive measures not only to detect and analyse security breaches in real time and mitigate any damage caused, but also upon aggressive countermeasures undertaken outside the victim network[4].

There are, however, a number of serious concerns with the implementation of active cyber defence (ACD) which will also be examined. There are questions regarding the legality of the use of aggressive countermeasures outside the defender's network, particularly by state actors. Such action can constitute armed attacks under international law which can be responded to with conventional military force. This in turn raises the issues of accurate attribution of incidents given the anonymising capacities of cyberspace, and the militarisation of cyberspace due to the involvement of state military and security apparatus in ACD measures.

To fully classify ACD, it is necessary to contextualise it with other approaches to cyber defence and security. In so doing, a more comprehensive and representative classification of active cyber defence will be made possible. However, this raises issues regarding the erroneous classification of non-ACD actions. Current analyses group together measures such as firewalls, good "cyber hygiene" and network resilience under the umbrella term "passive cyber defence"[5] – a mirror-image of active approaches. This term is not entirely accurate. A more nuanced classification of the actions collated under the term passive cyber defence will be proposed, categorising non-ACD measures as fortified cyber defence and resilient cyber defence.

Finally, it will be argued that the three approaches to cyber defence offered here do not operate in isolation from one another, as is implied by the use of dualistic terms such as "active" and "passive". An examination of the cyber security strategies of national actors will demonstrate that active, fortified and resilient cyber defence are employed in a collaborative triptych of approaches to cyber security: three independent but related concepts coming together to achieve the single goal of operating in cyberspace free from the risk of physical or digital harm.

3 A. Klimburg and H. Tiirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU* (European Parliament, April 2011), 11, http://www.europarl.europa.eu/committees/en/sede/studiesdownload.html?languageDocument=EN&file=41648; Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," *Mercatus Center at George Mason University*, 2011, 25, http://www.voafanti.com/gate/big5/mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

4 The definition includes measures associated with offensive action in cyberspace, also known as Computer Network Operations (CNO) or Computer Network Attack (CNA). See Sandro Gaycken, *Cyberwar: Das Internet als Kriegsschauplatz* (Munich, Germany: Open Source Press, 2011), 142; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, 1st ed. (CUP, 2012), 37. Gaycken also discusses deterrence, stating that "a good offense is often the best defence" (Gaycken, *Cyberwar*, 149.). Deterrence is not specifically addressed here as many of the deterring measures employed are active in nature, and based around maintaining a credible second strike in the event of an incident. See Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (2010): 69, doi:10.1080/09700160903354450; K. A. Taipale, "Cyber-Deterrence," *LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION, WARFARE, DIGITAL AND INTERNET IMMOBILIZATION*, January 1, 2009, 4, http://papers.ssrn.com/abstract=1336045.

5 James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," Survival 54, no. 4 (2012): 109; Leyi Shi et al., "Port and Address Hopping for Active Cyber-Defense," in *Intelligence and Security Informatics* (Springer, 2007), 295.

2. ACTIVE CYBER DEFENCE

Although the term "active defence" is common in the military as the idea of offensive action and counterattacks to deny advantage or position to the enemy[6], the concept remains elusive when applied to the cyber domain[7] and suffers a lack of clarity in related law and national policy[8]. A recent policy brief from the Center for North American Security argued that there is currently no commonly accepted definition of the term "active cyber defence"[9], missing an opportunity to provide one. Nevertheless, attempts have been made to define the concept. Rosenzweig offers a provisional definition as:

> "…the synchronized, real_time capability to discover, detect, analyze, and mitigate threats. [Active cyber defence] operates at network speed using sensors, software and intelligence to detect and stop malicious activity ideally before it can affect networks and systems."[10]

This definition identifies a number of features of ACD, the most important of which is the real-time detection and mitigation of key threats before damage occurs. Specific measures include the deployment of "white worms"[11], benign software similar to viruses but which seek out and destroy malicious software, identify intrusions[12] or engage in recovery procedures[13]. A second active defence tactic is to repeatedly change the target device's identity during data transmission, a process known as address hopping[14]. This has the dual role of masking the target's identifying characteristics as well as confusing the attacker[15]. Address hopping can serve as a useful action to counter espionage by masking the identities of devices where particular data is stored. Active cyber defence therefore places emphasis on proactive measures to counteract the immediate effects of a cyber-incident, either by identifying and neutralising malicious software or by deliberately seeking to mask the online presence of target devices to deter and counter espionage.

There are, however, a number of more aggressive measures which can be taken to defend systems and networks. While white worms can be used to seek out and combat malicious software, Curry and Heckman describe how they can also be used to turn the tools of hackers and would-be intruders against them and identify not just the attacking software, but the servers

6 Shane McGee, Randy V. Sabett, and Anand Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law* 8, no. 1 (2013): 206.
7 Farwell and Rohozinski, "The New Reality," 110.
8 McGee, Sabett, and Shah, "Adequate Attribution," 2.
9 Irving Lachow, *Active Cyber Defense: A Framework for Policymakers*, Policy Brief (Washington, DC: Center for North American Security, February 22, 2013), 3.
10 Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law* 47 (2013): 2.
11 Wenlian Lu, Shouhuai Xu, and Xinlei Yi, "Optimizing Active Cyber Defense," in *Decision and Game Theory for Security* (Springer, 2013), 207.
12 Dinniss, *Cyber Warfare*, 108.
13 Lu, Xu, and Yi, "Optimizing Active Cyber Defence," 210.
14 Shi et al., "Address Hopping," 295.
15 Keith A. Repik, *Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques* (DTIC Document, 2008), 22, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA488411.

and other hardware devices hosting and distributing the attacking code[16]. This is a process known as "hack-back"[17]. Once the source devices of an intrusion or attack have been identified steps can be taken to render those devices inoperative or otherwise prevent them from carrying out their goals. What makes these measures significant is that they are aggressive, offensive techniques which operate beyond the boundaries of the defender's network[18]. They are taking the fight to the attackers.

ACD is therefore a security paradigm employing two methods: one, the real-time identification and mitigation of threats in defenders' networks; two, the capacity to take aggressive, external offensive countermeasures. For the purposes of establishing, or at least beginning the process of developing, a lexicon of cyber security terminology, ACD can therefore be described as:

an approach to achieving cyber security predicated upon the deployment of measures to detect, analyse, 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.

Beyond the immediate purpose of establishing a definition of the term "active cyber defence" however, the concept of ACD as a combination of real-time detection and forceful external action raises four important concerns.

First, there are legal implications in the use of offensive external measures. Rosenzweig states that, within the United States (US), private companies are discouraged from using hack-backs as any unauthorised access to a computer or network violates the US Computer Fraud and Abuse Act[19]. This means that defenders who employ software to trace an attacking server and engage in retaliatory action in the attacker's network open themselves up to legal sanction as much as the initial attacker. Given that cyberspace is a series of global networks, this dubious legality is exacerbated when measures undertaken outside the victim network occur extra-territorially, i.e. across international borders[20]. Although such action, when carried out by private corporations, lacks legal cohesion and consensus[21] the concept is particularly problematic when the actors involved include nation-states rather than private companies[22].

The potential for the involvement of nation-states in aggressive cyber techniques is a serious problem because, according to Dinstein[23] and Schmitt[24], that involvement can constitute an armed attack if any action causes damage or disruption of "a scale…comparable to non-cyber

16 John Curry, "Active Defence," *ITNOW* 54, no. 4 (December 1, 2012): 26–27, doi:10.1093/itnow/bws103; Kristin E. Heckman et al., "Active Cyber Defense With Denial and Deception: A Cyber-Wargame Experiment," Computers & Security, 2013, 73, http://www.sciencedirect.com/science/article/pii/S016740481300076X.

17 McGee, Sabett, and Shah, "Adequate Attribution," 2; Rosenzweig, "International Law," 1.

18 Rosenzweig, "International Law," 3.

19 Ibid., 12.

20 Ronald J. Deibert, "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace," in *Routledge Handbook of Internet Politics*, ed. A. Chadwick and P. N. Howard (London: Routledge, 2009), 334.

21 Rosenzweig, "International Law," 13.

22 It should be noted that in certain circumstances, states are responsible for the actions of private companies, such as state-sponsored private actors or contractors.

23 Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," *Journal of Conflict and Security Law* 17, no. 2 (July 1, 2012): 261.

24 Michael N. Schmitt, "Classification of Cyber Conflict," *Journal of Conflict and Security Law* 17, no. 2 (July 1, 2012): 250.

operations"[25], has a trans-border element and the attributable involvement of another state and its armed forces[26]. Consequently, a hack-back can be construed as an armed attack if its purpose is to render inoperative the source of the attack and if its effects are comparable to the use of conventional force. This is significant because, under international law, such attacks can be responded to with a range of action including "forcible responses"[27]. This raises the spectre of incidents escalating beyond the cyber-domain into the physical domain. A policy precedent has already been set by the US in this regard. In 2011 policy was issued stating that the US reserved the right to respond to a cyber-attack with military force as the option of last resort[28]. Nation-states have the right to defend themselves against any forms of attack and this right extends beyond kinetic incidents to those perpetrated entirely through cyber operations[29]. However, utilising ACD as a policy or strategic choice must be considered carefully, given its inherent characteristic of action beyond the defender's immediate network[30].

Such risks raise a second problem when employing aggressive, extra-territorial measures: the accurate attribution of the initial incident given the anonymising capacity of cyberspace and its effects on accurately identifying perpetrators. Although the problem of attribution has been extensively examined[31] it is pertinent to raise it here to highlight a major pitfall with the application of ACD as a security strategy, especially given the possibility of kinetic responses to cyber incidents. The basic premise of the attribution problem is that one cannot know with 100% certainty that the identified origin location of a security breach is the true origin of that breach[32]. While attribution is not impossible the anonymising effect of the digital domain makes it very difficult and resource-intensive[33], a feature exploited by malicious online actors as a protection against identification. To respond to an intrusion with a damaging hack-back therefore requires a high degree of certainty. The defender must be confident that the identified source of an intrusion is the genuine source given the legal ramifications examined above. This need for certainty is increased exponentially if nation-states are allegedly involved and reserve the right to deploy conventional weapons as a response to a cyber-incident.

The involvement of state actors and their security and military apparatus leads to a third concern with the use of active cyber defence. Malicious activity in cyberspace runs a gamut from viruses that steal or delete personal data and engage in espionage to acts of sedition and

25 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), 45.

26 Schmitt, "Classification," 251; Schmitt, *Tallinn Manual*, 54. There is, however, currently an ongoing debate as to whether the actions described as "attacks" are in fact armed attacks or should more accurately be described as sabotage, subversion or espionage. In addition, very few incidents have occurred which qualify as attacks. See Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013) and Brandon Valeriano and Ryan Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11 (in Press)," *Journal of Peace Research*, 2014.

27 Dinniss, *Cyber Warfare*, 108.

28 USA, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, National Strategy (The White House, May 2011), 14, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

29 Schmitt, *Tallinn Manual*, 54.

30 Klimburg and Tiirmaa-Klaar, *Cybersecurity*, 13.

31 Dinniss, *Cyber Warfare*, 3,99; Gaycken, *Cyberwar*, 80–86; Schmitt, *Tallinn Manual*, 29–31; Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (2012): 229–44.

32 Dinniss, *Cyber Warfare*, 71.

33 Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," 233.

the publishing of extremist propaganda[34]. Certain online content is banned in certain states, and so the authorities in those states filter that content. However, Deibert and Rohozinski[35] argue that there is the potential for a "mission creep" to set in when a state deploys the tools necessary to detect malicious activity before it causes any adverse effects. They cite the example of a crackdown on internet pornography by the Thai government leading to the complete blocking of access to YouTube.com[36] as a warning that, once the tools such as filters, address blocking and content analysis are in place, there is a great temptation to employ these tools for an ever expanding range of purposes. The allegations of mass surveillance of digital communications by Western security services published in the UK's Guardian newspaper[37] in 2013 demonstrate the risks of such a mission creep. What began as measures to combat terrorism have allegedly become programmes of mass data collection. The point here is that the use of ACD measures must be carried out with great care to avoid expanding a filtering remit beyond legitimate security concerns – such as preventing the spread of extremist propaganda – to overzealous measures such as unauthorised access to private correspondence.

The problem with such active filtering and surveillance is that, given the opportunities for the deployment of state apparatus[38], these actions are often carried out by national security or military institutions, leading to a potential militarisation of cyberspace[39]. The cyber security strategies of the actors adopting an ACD approach demonstrate the level to which military institutions are already being deployed as part of the security solution. In two specific cases – namely United Kingdom (UK) and the US – military institutions play a strong role in providing and ensuring cyber security though active cyber defence measures.

The UK Cyber Security Strategy identifies the proactive measures taken to disrupt threats to and from networked communications systems[40]. The Ministry of Defence (MoD) is tasked with improving the UK's ability to detect threats in cyberspace and to "anticipate, prepare for and disrupt" such threats[41]. To do this, resources have been provided to the MoD itself and the Government Communications Headquarters (GCHQ) to develop a range of techniques – including proactive measures – to disrupt those threats. This strategic approach falls neatly into Rosenzweig's definition of ACD – efforts to detect and hinder malicious activity – but implies the extension of action beyond the confines of national or UK government networks through proactive measures described by Curry and Heckman, as well as Lu et al[42]. The fact that the MoD has been assigned these tasks, despite UK cyber security strategy being led by the Cabinet

34 Maura Conway, "Cybercortical Warfare: Hizbollah's Internet Strategy," in *The Internet and Politics; Citizens, Voters and Activist*s, ed. S. Oates, D. Owen, and R. Gibson (Routledge, 2005); Jialun Qin et al., "Analyzing Terror Campaigns on the Internet: Technical Sophistication, Content Richness, and Web Interactivity," *International Journal of Human-Computer Studies* 65, no. 1 (January 2007): 71–84.

35 Deibert, "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace," 327.

36 Ibid.

37 The Guardian, "The NSA Files," Report Series, *The NSA Files | World News | The Guardian*, June 8, 2013, http://www.guardian.co.uk/world/the-nsa-files.

38 Curry, "Active Defence."

39 Ronald J. Deibert, "Militarizing Cyberspace," *Technology Review* 12 (August 2010), http://www.technologyreview.com/notebook/419458/militarizing-cyberspace/; Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," in *4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (NATO CCD COE Publications, 2012), 141–53.

40 UK, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, National Strategy (UK Cabinet Office, 2011), 27.

41 Ibid., 39.

42 Curry, "Active Defence"; Heckman et al., "Active Cyber Defense With Denial and Deception"; Lu, Xu, and Yi, "Optimizing Active Cyber Defence."

Office – a civilian organ of central government – demonstrates a willingness to deploy military resources to provide cyber defence and security.

Such willingness is also present in the US's approach to cyber security. There are two documents which together expound American policy in this field: the White House's International Strategy for Cyberspace[43] and the Department of Defense (DoD)'s Strategy for Operating in Cyberspace[44]. The second document specifically cites the use of active cyber defence capabilities to prevent intrusions[45], clearly placing it within an active framework. Furthermore, as examined above, the prominence of military institutions in US cyber security policy and strategy is demonstrated by the explicit willingness of the American government to use military force (when all other avenues have been exhausted) in response to hostile acts in cyberspace[46]. If a key principle of ACD is the extension of measures beyond the immediate confines of victim systems and networks, then the use of kinetic military force in response to a cyber-attack is the ultimate example of such an extension and the example most prone to the issues of legality, attribution, mission creep and militarisation. Clearly therefore, the adoption of such active defence policies is concerning as it means military resources are being deployed to ensure security[47], necessarily increasing the level to which national military and security services are involved in cyber security policy decisions. Cyberspace has already been classified as a fifth military domain by the US and Japan[48] leading these states to seek military capacities and capabilities in that domain. The mission creep Deibert and Rohozinski warned against is manifesting itself in an increased military presence in cyberspace particularly if it takes on the task not only of restricting access to particular data, but also engages in measures outside the home networks of defended states.

The concept of combatting threats outside the network or systems under attack therefore raises a number of significant concerns, not least the capacity for defending actors to respond with kinetic military force and the ramifications of doing so. However, the extra-territoriality inherent to ACD is vital to our understanding of the concept as a methodological approach to cyber security due to the fact that it is this aggressive external action which differentiates ACD from other approaches. These other approaches have to date been described as "passive cyber defence"[49]. Such a description raises a fourth issue around ACD and current efforts to define the concept: the assumption that all other, non-active forms of cyber defence are "passive" or reactive in nature.

Farwell and Rohozinski describe passive cyber defence as an approach which includes:

> "firewalls, cyber 'hygiene' that trains an educated workforce to guard against errors or transgressions that can lead to cyber intrusion, detection technology, 'honey pots' or

43 USA, *International Strategy*.

44 USA, *Department of Defense Strategy for Operating in Cyberspace*, National Strategy (Department of Defense, 2011), http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

45 Ibid., 6.

46 USA, *International Strategy*, 14.

47 Dunn Cavelty, "Militarisation of Cyberspace," 141; Ronald J. Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium-Journal of International Studies* 32, no. 3 (2003): 501–30.

48 Japan, "Cyber Security Strategy of Japan," June 2013, 41, http://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf; USA, *Strategy for Operating in Cyberspace*, 5.

49 Farwell and Rohozinski, "The New Reality," 109; Shi et al., "Address Hopping," 295.

> decoys that serve as diversions, and managing cyberspace risk through collective defence, smart partnerships, information training, greater situation awareness, and establishing secure, resilient network environments"[50]

Such actions, as well as installing intrusion detection and prevention measures[51] are not considered active defences. Rather they create a preventive environment[52] predicated on information-sharing and resilience. Lachow goes further, arguing that passive cyber defences which rely on perimeter sensors cannot adequately protect against sophisticated cyber-attacks[53] as these can adapt quickly and become more advanced than the defences of their targets. The term "passive" therefore implies a purely reactive approach: dealing with an incident once it has occurred rather than actively trying to prevent that occurrence in the first place. However, just as ACD is not as simple as taking proactive action of any kind, the construction of decoys, collective defence paradigms, information-sharing and the development of resilient networks which can cope with accidental or intentional damage are not simple reactions, and certainly not passive policies. They involve taking action to prevent and minimise the damage of a cyber-incident without resorting to the aggressive measures inherent to ACD.

In the interests of developing a consistent, coherent lexicon of terminology, active cyber defence is not the only term that suffers from a lack of definition. The same is true of that group of measures taken to mitigate the damage of cyber-incidents or return systems and networks to full functionality in the event of an incident. Instead of labelling these measures "passive cyber defence" – a simple mirror-image of "active cyber defence" – a clearer and more accurate categorisation of these measures would be to label them "fortified cyber defence" and "resilient cyber defence".

3. FORTIFIED CYBER DEFENCE

As discussed above, measures such as the establishment of firewalls, anti-virus software and detection technologies have been labelled by some commentators as passive, reactive forms of defence. However, if the ultimate aim of these actions is examined, the collection of measures involved cannot be accurately labelled as passive. The goal of firewalls and filters, and any other measures intended to prevent malicious access to key assets is just that – the prevention of access[54]. Steps are taken to reduce the chances of any intrusion or attack succeeding in its aims. An analogy to this is the construction of physical fortifications such as castles and fortresses. These were built with the intention of protecting those inside from outside attackers. Methods such as installing firewalls or placing filters and scanners on trunk cables are all intended to prevent malicious code, information or actors accessing network systems and exploiting assets[55]. These are not "passive" measures, taken in reaction to an incident; rather they are actions designed to build virtual fortifications.

In addition to the installation of firewalls and anti-virus software, fortified cyber defence (FCD)

50 Farwell and Rohozinski, "The New Reality," 109.
51 Shi et al., "Address Hopping," 295.
52 Lu, Xu, and Yi, "Optimizing Active Cyber Defence," 209.
53 Lachow, *Active Cyber Defense*, 1.
54 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 25, doi:10.1111/j.1749-5687.2009.00088.x.
55 Deibert, "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace," 325.

can be achieved by building security into the infrastructure supporting cyberspace: the software, computers, routers and other elements needed to enable the online domain to function[56]. The unpredictable and fragile nature of vast international computer networks creates a systemic ontological insecurity in cyberspace[57], making its infrastructure vulnerable to natural, accidental or malicious incidents. Data packets can be corrupted while in transit due to faulty cables, individual computers can themselves malfunction over time and software can fail. Building security measures into all the elements required for the international communications networks to function would mitigate against such systemic and exploitable vulnerabilities. In addition to providing a definition of active cyber defence, a definition of FCD is also offered here:

constructing systemically secure communications and information networks in order to establish defensive perimeters around key assets and minimise intentional or unintentional incidents or damage.

While the defining characteristic of ACD is aggressive action taken outside the defender's home network, the defining characteristic of FCD is that approach's preventive, introspective focus. FCD measures seek to establish defensive perimeters through systems of firewalls and antivirus software in order to minimise the chances of access to target systems and networks.

As discussed above, the US and UK cyber security strategies provide examples of national policies adopting ACD. Germany, on the other hand, provides an example of a national policy promoting FCD[58]. The focus for the German Cyber Security Strategy is ensuring that malicious intrusions are unsuccessful within a preventive security framework[59]. This is achieved through certain key objectives, including training and international co-operation as well as tackling cyber-crime. The ultimate aim of the German Strategy is to ensure that critical infrastructures and public and private IT systems are secure from threats which affect the confidentiality, integrity and availability of electronic data, and the availability of information and communications technology (ICT)[60]. The German approach to cyber security is therefore not a passive, reactive approach despite employing techniques Farwell and Rohozinski associate with passive cyber defence[61]. It is proactive in that it takes the issues seriously and aims to put in place particular measures to create a preventive environment where the possibility of breach success is minimised while not employing aggressive extra-territorial countermeasures designed for operation in an attacker's home network.

4. RESILIENT CYBER DEFENCE

A third approach to cyber defence is based not upon aggressively seeking perpetrators of security breaches or establishing fortifications around key assets. Instead it focusses on ensuring critical

56 Gary McGraw, "Cyber War Is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies* 36, no. 1 (February 2013): 113.

57 Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1160.

58 Germany, *Cyber Security Strategy for Germany (official Translation)*, National Strategy (Bonn: Federal Office for Information Security, 2011), http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.html?nn=109632.

59 Ibid., 5.

60 Ibid., 4.

61 Farwell and Rohozinski, "The New Reality," 109.

infrastructures and services which rely on networked communications continue to function and to provide the services for which they were designed. Rather than aggressive or fortified cyber defence, a potentially more pragmatic approach to cyber security in general is "resilient cyber defence" (RCD).

Resilience itself is predicated upon accepting that incidents will occur and focussing on the ability to recover from those incidents[62], either returning to the original state or adapting to generate a new, adjusted state[63]. In terms of precise technical measures, resilience in the cyber domain shares a number of traits with FCD: it requires practitioners and policy makers to focus their security efforts internally, making sure systems and networks are adaptable or can withstand incidents. Building security measures into those systems[64] is a key feature in such preparedness. RCD can therefore be defined as:

ensuring the continuity of system functionality and service provision by constructing communications and information networks with the systemic, inbuilt ability to withstand or adapt to intentional or unintentional incidents.

While ACD and FCD seek to identify threats and intrusions as soon as possible and deal with them, RCD advocates sharing vital information regarding security breaches among all interested parties and potential future victims[65].

Resilience is a common trait in current cyber security policy documents. The strategies of the European Union (EU) and Japan favour this approach. They concentrate on sharing information between public and private bodies, harmonising public infrastructure security measures and developing uniform standards of security[66] to ensure preparedness in the event of a natural or malicious incident. Other features of resilient cyber defence include ensuring that the private sector is actively involved in solution development, and promoting the recognition of shared responsibility amongst government agencies, private companies and individual users. That way, as many actors as possible know of a particular virus or intrusion mechanism and can take steps to ensure that system functionality continues should they be targeted.

The defining characteristic of RCD is this idea of functional continuity. Active paradigms concentrate on identifying threats and their origins and taking remedial and punitive external action. Fortified models focus on ensuring that network defences are in place to prevent, or at least minimise the success of, a security breach. Resilient models prioritise the continued functioning and service provision of the systems that rely on network communications so that

62 Christopher W. Zobel and Lara Khansa, "Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks," *Decision Sciences* 43, no. 4 (2012): 688.

63 Myriam Dunn Cavelty, "Cyber-Security," in *Contemporary Security Studies*, ed. Alan Collins, 3rd ed. (OUP, 2012), 19.

64 Hansen and Nissenbaum, "Digital Disaster"; McGraw, "Cyber War."

65 European Commission, *JOIN (2013) 1 Final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Communication (European Commission, February 7, 2013), 6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:pdf.

66 Japan, "Cyber Security Strategy," 30; European Commission, *Cybersecurity Strategy*, 5.

there is no break in that service[67]. To provide a simple example: if a power station suffers a cyber security breach, the first priority for an RCD approach would be to ensure that electricity production continues unaffected.

On examination therefore, fortified and resilience-based cyber defence solutions cannot be described as "passive cyber defence"[68]. Rather, they advocate a state of readiness, a capability to withstand malicious or natural incidents. Processes and procedures must be put in place to involve all interested actors in information-sharing, whether these are government agencies, public bodies or private sector companies. The EU is currently considering legislation which would make it a legal requirement for all relevant public and private actors to share security breach information[69]. Network fortification and resilience recommends that security and adaptability be built into the infrastructure supporting the online environment[70]. Given that cyber-incidents are varied and increasing[71], a state of readiness is a far more pragmatic option than aggressive techniques fraught with issues around accurate attribution, questionable legal standpoints and overzealous deployment of security and military resources and the consequences those actions risk.

The result of this classification is the identification of not two modes of cyber defence (active or passive), but three – active, fortified and resilient cyber defence. However the three paradigms are not mutually exclusive. While very different given their varying techniques, each approach operates in conjunction with the other to achieve a wider single goal, cyber security. By concentrating not on the implementation of the measures themselves but their ultimate goals these three paradigms together form a "Triptych of Cyber Security": three parallel approaches to achieving security when interacting with and utilising cyberspace.

5. CONCLUSION – THE "TRIPTYCH" OF CYBER SECURITY

Active cyber defence (ACD) is an approach to cyber security predicated upon proactive measures to identify malicious codes and other threats, as well as aggressive external techniques designed to neutralise threat agents. ACD is defined by the capacity and willingness to take action outside the victim network[72]. Despite this, ACD is not mirrored by "passive cyber defence". The measures collated under this term should more accurately be classified as fortified and resilient cyber defence. These terms clarify the nature of the action taken by focussing on the end goals of the measures they describe.

The three types of cyber defence described here are not mutually exclusive. Instead they operate

67 European Commission, *Cybersecurity Strategy*, 6; Switzerland, *National Strategy for Switzerland's Protection against Cyber Risks*, National Strategy, 2012, 38, http://www.melani.admin.ch/dokumentation/00123/01525/index.html?lang=en.

68 Farwell and Rohozinski, "The New Reality," 109; Lachow, *Active Cyber Defense*, 1; Shi et al., "Address Hopping," 295.

69 European Commission, "COM (2013) 48 Final Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union" (EUR-Lex, February 7, 2013), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF.

70 McGraw, "Cyber War."

71 European Commission, *Cybersecurity Strategy*, 3.

72 Lu, Xu, and Yi, "Optimizing Active Cyber Defence"; Rosenzweig, "International Law," 3.

in conjunction with one another in a triptych of measures further highlighting the inaccuracy of a simple divide between active and passive approaches. The goal of cyber security is to enable operations in cyberspace free from the risk of physical or digital harm. To that end, the three paradigms of defence postulated here work together to complement each other through a range of measures designed to address specific issues around online security. Active cyber defence focusses on identifying and neutralising threats and threat agents both inside and outside the defender's network, while fortified defence builds a protective environment. In its turn resilience focusses on ensuring system continuity. The national strategies developed over the last ten years demonstrate the complementarity of these three approaches. The US and UK categorically adopt an active paradigm, whereby all available resources are deployed to protect national interests, including proactively seeking out enemy actors and rendering them ineffective. The US further retains the right to deploy the ultimate sanction of kinetic military force in the event of a cyber-attack as a measure of last resort. However, neither the UK nor the US are ignorant of the benefits of fortifying assets, or of making critical national infrastructures resilient to the failures of the communications systems on which they rely[73]. For Germany the policy of choice is FCD but network resilience is recognised in a commitment to protecting and securing critical digital infrastructures due to their importance to physical social and economic services[74]. The EU and Japan adopt a resilience-based framework, yet both are seeking to develop active defence capabilities[75].

What this demonstrates is a conscious acknowledgement that one single approach to cyber security is not enough. Active cyber defence, including all the measures that that concept entails, is insufficient when seeking to achieve cyber security. Steps must be taken to fortify assets in order to minimise the likelihood and effectiveness of cyber-incidents, as well as ensure system and infrastructure continuity should an incident occur. Equally, FCD and RCD do not serve as effective deterrents to would-be attackers. The willingness to identify and pursue threat agents into their own home networks must be demonstrated alongside asset fortification and system resilience. In short, the paradigms of cyber defence are not stand-alone approaches. Even for those actors which place their strategies within an active framework, military or security agency resources are not the only ones utilised. The consequence of this is the deployment of elements of each approach simultaneously in a triptych of approaches intended to achieve a single goal.

By contextualising ACD as an approach which is used collaboratively with its fortified and resilient cousins in a triptych of cyber security, and highlighting the crucial difference of aggressive action beyond the victim network, it is possible to distil a definition of the term "active cyber defence". This is in spite of ACD being fraught with unresolved legal and diplomatic difficulties. For the purposes of classification, a definition of active cyber defence is proposed here:

a method of achieving cyber security predicated upon the deployment of measures to detect, analyse, identify and mitigate threats to and from cyberspace in real-time, combined with the capability and resources to take proactive or aggressive action against threat agents in those agents' home networks.

73 UK, *Cyber Security Strategy*, 39; USA, *Strategy for Operating in Cyberspace*, 6; USA, *International Strategy*, 18.
74 Germany, *Cyber Security Strategy*, 6.
75 European Commission, *Cybersecurity Strategy*, 11; Japan, "Cyber Security Strategy," 41.

The question of definition and classification in the cyber security debate will not be resolved overnight. While active cyber defence is one feature of that debate, the definition and classification offered here will go some way towards establishing a cohesive lexicon of terminology, an exercise which will assist the development of legal and political solutions to the complex issue of cyber security.

REFERENCES:

Conway, Maura. "Cybercortical Warfare: Hizbollah's Internet Strategy." In *The Internet and Politics; Citizens, Voters and Activists*, edited by S. Oates, D. Owen, and R. Gibson. Routledge, 2005.

Curry, John. "Active Defence." *ITNOW* 54, no. 4 (December 1, 2012): 26–27. doi:10.1093/itnow/bws103.

Deibert, Ronald J. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium-Journal of International Studies* 32, no. 3 (2003): 501–30.
"Militarizing Cyberspace." *Technology Review* 12 (August 2010). http://www.technologyreview.com/notebook/419458/militarizing-cyberspace/.
"The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace." In *Routledge Handbook of Internet Politics*, edited by A. Chadwick and P. N. Howard, 323–36. London: Routledge, 2009.

Deibert, Ronald J., and Rafal Rohozinski. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4, no. 1 (2010): 15–32. doi:10.1111/j.1749-5687.2009.00088.x.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. 1st ed. CUP, 2012.

Dinstein, Yoram. "The Principle of Distinction and Cyber War in International Armed Conflicts." *Journal of Conflict and Security Law* 17, no. 2 (July 1, 2012): 261–77. doi:10.1093/jcsl/krs015.

Dunn Cavelty, Myriam. "Cyber-Security." In *Contemporary Security Studies*, edited by Alan Collins. 3rd ed. OUP, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055122.
"The Militarisation of Cyberspace: Why Less May Be Better." In *4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski, 141–53. NATO CCD COE Publications, 2012.

European Commission. "COM (2013) 48 Final Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union." EUR-Lex, February 7, 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF.
JOIN (2013) 1 Final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Communication. European Commission, February 7, 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:pdf.

Farwell, James P., and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4 (2012): 107–20.

Gaycken, Sandro. *Cyberwar: Das Internet als Kriegsschauplatz*. Munich, Germany: Open Source Press, 2011.

Germany. *Cyber Security Strategy for Germany (official Translation)*. National Strategy. Bonn: Federal Office for Information Security, 2011. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.html?nn=109632.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, no. 4 (2009): 1155–75. doi:10.1111/j.1468-2478.2009.00572.x.

Heckman, Kristin E., Michael J. Walsh, Frank J. Stech, Todd A. O'Boyle, Stephen R. DiCato, and Audra F. Herber. "Active Cyber Defense With Denial and Deception: A Cyber-Wargame Experiment." *Computers & Security*, 2013. http://www.sciencedirect.com/science/article/pii/S016740481300076X.

Japan. "Cyber Security Strategy of Japan," June 2013. http://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf.

Klimburg, A., and H. Tiirmaa-Klaar. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. European Parliament, April 2011. http://www.europarl.europa.eu/committees/en/sede/studiesdownload.html?languageDocument=EN&file=41648.

Kruger, Dan. "Radically Simplifying Cybersecurity," 2012. http://www.absio.com/sites/default/files/assets/Radically_Simplifying_Cybersecurity_V1.4_1.pdf.

Lachow, Irving. *Active Cyber Defense: A Framework for Policymakers*. Policy Brief. Washington, DC: Center for North American Security, February 22, 2013. http://www.cnas.org/publications/policy-briefs/active-cyber-defense-a-framework-for-policymakers.

Lawson, Sean. "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History." *Mercatus Center at George Mason University*, 2011. http://www.voafanti.com/gate/big5/mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

Lu, Wenlian, Shouhuai Xu, and Xinlei Yi. "Optimizing Active Cyber Defense." In *Decision and Game Theory for Security*, 206–25. Springer, 2013. http://link.springer.com/chapter/10.1007/978-3-319-02786-9_13.

McGee, Shane, Randy V. Sabett, and Anand Shah. "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense." *Journal of Business & Technology Law* 8, no. 1 (2013): 1.

McGraw, Gary. "Cyber War Is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36, no. 1 (February 2013): 109–19. doi:10.1080/01402390.2012.742013.

Qin, Jialun, Yilu Zhou, Edna Reid, Guanpi Lai, and Hsinchun Chen. "Analyzing Terror Campaigns on the Internet: Technical Sophistication, Content Richness, and Web Interactivity." *International Journal of Human-Computer Studies* 65, no. 1 (January 2007): 71–84. doi:10.1016/j.ijhcs.2006.08.012.

Repik, Keith A. *Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques*. DTIC Document, 2008. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA488411.

Rid, Thomas. *Cyber War Will Not Take Place*. London: Hurst, 2013.

Rosenzweig, Paul. "International Law and Private Actor Active Cyber Defensive Measures." *Stanford Journal of International Law* 47 (2013). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2270673.

Schmitt, Michael N. "Classification of Cyber Conflict." *Journal of Conflict and Security Law* 17, no. 2 (July 1, 2012): 245–60. doi:10.1093/jcsl/krs018.
, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. CUP, 2013.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34, no. 1 (2010): 62–73. doi:10.1080/09700160903354450.

Shi, Leyi, Chunfu Jia, Shuwang Lü, and Zhenhua Liu. "Port and Address Hopping for Active Cyber-Defense." *In Intelligence and Security Informatics*, 295–300. Springer, 2007. http://link.springer.com/chapter/10.1007/978-3-540-71549-8_31.

Switzerland. *National Strategy for Switzerland's Protection against Cyber Risks*. National Strategy, 2012. http://www.melani.admin.ch/dokumentation/00123/01525/index.html?lang=en.

Taipale, K. A. “Cyber-Deterrence.” *LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION, WARFARE, DIGITAL AND INTERNET IMMOBILIZATION*, January 1, 2009. http://papers.ssrn.com/abstract=1336045.

The Guardian. “The NSA Files.” Report Series. *The NSA Files | World News | The Guardian*, June 8, 2013. http://www.guardian.co.uk/world/the-nsa-files.

Tsagourias, Nicholas. “Cyber Attacks, Self-Defence and the Problem of Attribution.” *Journal of Conflict and Security Law* 17, no. 2 (2012): 229–44.

UK. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. National Strategy. UK Cabinet Office, 2011. http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy.

USA. *Department of Defense Strategy for Operating in Cyberspace*. National Strategy. Department of Defense, 2011. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.
International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. National Strategy. The White House, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Valeriano, Brandon, and Ryan Maness. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11 (in Press).” *Journal of Peace Research*, 2014.

Zobel, Christopher W., and Lara Khansa. “Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks.” *Decision Sciences* 43, no. 4 (2012): 687–710.