A Conceptual Review of Cyber-Operations for the Royal Navy

Sub Lieutenant Christopher Argles RN
Edited by Ed Zaluska

ABSTRACT

Cyberspace is a malleable and seemingly ubiquitous environment through which information flows. Armed forces use this information to make decisions and take action. The fundamental importance of cyberspace to modern military operations leads threat actors to desire access to and control over its components. In response, organizations like the Royal Navy conduct defensive Cyber-Operations (CO) to protect their information networks and platforms. At the same time, offensive CO allow armed forces to take advantage of the reach of cyberspace to weaken the position of their adversaries. This paper discusses the nature of the threats faced by national-security institutions, and the doctrinal factors that policy-makers must consider. The paper reviews the approach to CO of several countries and evaluates the work done by the Royal Navy in developing cyber capabilities.

I. INTRODUCTION ABSTRACT

1.1 Problem statement

Little information exists in the public domain about any of the Cyber-Operations (CO) conducted by the British Armed Forces. The sensitive nature of the deployment of cyber capabilities for military purposes requires that access to these details remains under tight restrictions. Nevertheless, a few publications by the Ministry of Defence (MOD) provide an insight into the approach to CO adopted by the Armed Forces. This material discloses some of the high-level concepts about training, organizational structures, and policy.

Sub Lieutenant Christopher Argles serves as a Junior Officer in the Weapons Engineering branch of the Royal Navy. Sub Lieutenant Argles joined the Royal Navy as a Midshipman under the Defence Technical Undergraduate Scheme in 2013. In 2016 he spent a period attached to the Information Directorate of the United States Air Force Research Laboratory to research information assurance and deception in contested cyber environments. He graduated from the University of Southampton with a Master's Degree in Computer Science with Cyber Security. Upon receipt of his commission from Britannia Royal Naval College, he was selected to join the Submarine Service and undertook the Weapon System Engineering and Management Course at HMS COLLINGWOOD. In his current role, Sub Lieutenant Argles supports maritime C4ISR operations.

A discussion of the ideas presented by the MOD, and a comparison of the UK approach with that of other countries, provides an insight into the evolution of current doctrine. However, there appears to be very little evidence of this in the open literature.

This paper draws upon several cyber reports, policy documents, and academic papers to highlight some of the key factors that affect CO and to set out recommendations for policy-makers to consider. The Royal Navy is selected as the focus of this paper because of the challenges associated with the conduct of maritime CO, in addition to the author's background as a Naval Officer. Interviews with members of the Royal Navy's new Cyber Defence Operations Centre (CDOC) and attendance at INFORMATION WARRIOR 17 (IW 17) enable this paper to provide a privileged evaluation of the work undertaken by the Royal Navy in implementing the tactics, techniques, and procedures required to deliver an operational cyber capability.

1.1 Contributions

Section 2 presents a background to current threats and threat actors in cyberspace and discusses how they affect national security. This section also highlights the need for policy-makers to understand the type of randomness that applies to CO. Section 3 summarizes the approach to CO adopted by the United States Department of Defense (DoD), China, and Russia. The report then provides an overview of the work done by the United Kingdom and the Royal Navy in the development of CO doctrine and capability. Section 4 looks at how the Royal Navy recruits and trains the individuals who serve in cyber roles. Moreover, the section details the potential contribution that "Capture the Flag" (CTF) competitions might make towards improving the preparedness of cyber personnel. From the evaluations in Section 3 and 4, the report sets out several recommendations to inform future discussions on Royal Navy CO doctrine.

Ed Zaluska is an Associate Professor in Electronics and Computer Science at the University of Southampton (UK) and a Life Senior Member of the IEEE. His current research interests embrace cybersecurity and all security aspects associated with distributed systems.

1.3 Limitations

This paper provides an open review in the unclassified domain of the CO doctrine of several major powers, intended for cyber policymakers and CO researchers. Specific details about technical capabilities and associated deployments remain outside the scope of this evaluation. Because of this, some of the conclusions and recommendations presented in this report might not apply in full to the Royal Navy but should be interpreted as proposed guidelines and principles for future consideration.

2. BACKGROUND

2.1 Definitions

While many definitions of cyberspace exist, this report (unless specified in the context of national doctrine) uses the definition provided by Ormrod and Turnbull:

> "an evolving loosely bounded and interconnected information environment that utilizes technologically mediated software-enabled methods of communication" [1]. As defined in the MOD Cyber Primer, CO refers to "activities that project power to achieve military objectives in, or through, cyberspace" [2].

2.2 Current threats

Alongside terrorism, and interstate conflict, the 2015 Strategic Defence and Security Review listed cyber threats to the United Kingdom and her interests as a 'Tier One' (highest priority) risk to national security [3]. As computer technologies and information networks continue to increase across naval platforms (ships, submarines, etc.) and supportive infrastructure (information services, logistics, education, etc.), the Royal Navy becomes ever more dependent on the assured functionality of these systems [4].

Muti and Tajer provide some real-world and hypothetical scenarios to illustrate the types of CO which threaten national security institutions like the Royal Navy [5]. Their report cites a consensus among scholars that the impact of CO on national security is often exaggerated [6]. We wish to highlight those CO that pose a genuine threat.

The most serious concern is the discovery of vulnerabilities in the Supervisory Control and Data Acquisition (SCADA) technology used in Critical National Infrastructure (CNI) and in military platforms that provide an interface between a user and machinery. The report describes how these vulnerabilities facilitate the use of sabotage CO by state-supported threat actors. The Stuxnet operation [7], for example, used four zero-day (previously unknown vulnerability) exploits against the centrifuge SCADA system of the Iranian uranium enrichment facility at Natanz. The covert nature of Stuxnet meant that the scientists at the facility could not explain what caused the enrichment to fail. Muti and Tajer suggest that this undermined the trust the Iranian government placed in the abilities of the scientists.

In contrast, overt CO allows a state-supported threat actor to demonstrate their capabilities as a deterrent towards potential adversaries. The report speculates that in war, destructive CO against the SCADA systems of CNI (energy infrastructure, transport networks, hospitals, etc.) might result in catastrophic effects, e.g., significant loss of life. However, the technical complexity and the substantial resources required by them mean that, at present, such operations remain the preserve of state-supported threat actors.

The report also describes how nations conduct CO to augment traditional military operations. The authors cite a 2007 Israeli bombing raid, Operation Orchard, on a Syrian nuclear reactor site, to illustrate the vulnerability of military command and control networks. In this instance, the exploitation of the Syrian air defense information network and the subsequent creation of spoofed traffic allowed the free passage of the Israeli aircraft to and from their target [8]. Another example occurred during the Russo-Georgian conflict in 2008. Here, Russia conducted low-level CO against web-based financial and governmental services in Georgia prior to the launch of a ground offensive. The operation caused significant disruption to the lives of Georgian citizens and affected the ability of the government to coordinate a response.

Like the Georgian experience, Estonia fell victim to a Distributed Denial of Service (DDoS) CO against the web services of banks and the government. Again, the attack originated from Russia, but on this occasion, the perpetrators stated that they formed part of a government-financed youth collective known as Nashi. The Estonian government was unable to respond in-kind against the Russian government or to invoke the collective defense clause of the North Atlantic Treaty Organization (NATO) (Article 5). In response, Estonia established the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). This organization produced the Tallin Manual on International Law Applicable to Cyber Operations, which proposes that financial support of a threat actor by a state does not constitute

'overall control' of the CO conducted by that actor [9]. The absence of a normative international framework that addresses the ambiguity that exists in the relationship between states and state-sponsored, threat actors, creates opportunities for CO to occur without the risk of proportionate retaliation.

In their report, Muti and Tajer use the example of China's efforts in 2013 to disrupt an investigation by the *New York Times* into China's Prime Minister to illustrate how threat actors seek to control public perception. Analysis by the cybersecurity firm Mandiant [10] described how spear phishing e-mails sent to *New York Times* employees contained malicious attachments which, once opened, provided remote backdoor access to their work computers. To disguise the source of the activity, the operation was conducted through compromised proxy hosts in the United States. Once into the system, they escalated their user account privilege to pivot laterally onto other hosts on the network where they exfiltrated sensitive information. This process of compromise-persist-escalate-pivot-compromise forms a standard lifecycle for CO referred to in the cybersecurity community as Advanced Persistent Threat (APT) [11].

One area Muti and Tajer failed to illustrate is the internal threat. The unauthorized public disclosure by Edward Snowden of 1.5 million documents demonstrates the potential damage that can be caused by trusted users. A report by the United States House of Representatives referred to the leak of classified information by the former National Security Agency contractor as "the most damaging [...] in history" [12].

2.3 Power-laws in cyber-operations

In his article, *How Power-Laws Re-Write the Rules of Cyber Warfare*, Bibighaus describes the fundamental assumption that exists amongst strategic thinkers that, in warfare, Armed Forces shall operate in environments defined by Gaussian randomness [13]. Instead, the author argues that in CO, a different type of randomness, governed by Power-Law distribution, exists.

In Gaussian random environments such as the physical world, the factor by which events deviate from the norm is low. Bibighaus cites the example of human height; where the tallest man alive stands at 8'3", 1.5 times taller than the average. In Power-Law random environments such as personal wealth, a handful of events occur that deviate by a massive factor from the norm. For instance, the author compares the wealth of Bill Gates to that of the average person. The philosopher Nicholas Taleb describes the occurrence of these rare but powerful events as Black Swans. Bibighaus notes that Power-Law distributions follow the Pareto principle, whereby 80% of the impact derives from 20% of the causes [14].

In CO, Power-Law randomness manifests itself in several ways. For example, while the vast majority of malicious exploits (or 'cyber-weapons') created pose little or no threat, a few are highly damaging. Bibighaus highlights how a single virus, Conficker.B, infected millions of systems as evidence to that effect. Related to this, the author describes how the Power-Law distribution applies to the number of requests made by programs to software libraries. Programs depend on the integrity of these libraries. When threat actors exploit a major software library, large numbers of programs become vulnerable.

The article describes how these rare but powerful exploits require a cyber warrior of exceptional talent to create them. From this, Bibighaus stresses that talent rather than the mass of numbers serves as the primary measure of power in CO. Therefore, the recruitment and retention of gifted 'cyber warriors,' and the fundamental requirement for quality over quantity presents an additional factor for policy-makers to consider.

3. APPROACHES TO CYBER-OPERATIONS

3.1 United States

The 2015 DoD cyber strategy sets out the activities that the US armed forces shall undertake to develop a coherent CO capability [15]. The DoD defines cyberspace as an operational sub-domain within the information environment, formed of technology infrastructures and data [16]. The allocation of 'domain' status to cyberspace (alongside maritime, land, air, and space) serves a bureaucratic purpose to ensure that CO receives sufficient financial and material support.

The strategy calls for a national endeavor to defend against the CO of adversarial threat actors. To achieve this, the DoD lists five strategic goals: force readiness, information assurance, defensive operations, offensive operations, and deterrence. A 6,200 strong 'Cyber Mission Force (CMF)' shall deliver these goals. The CMF is comprised of 133 teams and is subdivided into the 'Combat Mission Force' (CO in support of operations), 'National Mission Force' (to counter significant cyber threats) and 'Cyber Protection Force' (to defend against day-to-day cyber threats). The DoD aims to establish a capability to model and simulate CO, enabling a regular pattern of network defense exercises to take place. This serves to address the need to train and prepare those individuals involved in CO and prevents the skill-fade that occurs after periods of inaction. Furthermore, the establishment of viable CO career paths shall help retain talented personnel.

The strategy discusses the need to learn from the experience of the private sector, a body that accounts for more than 90% of US network infrastructure. Commercial Computer Emergency Response Teams (CERTs) have found that continuous defensive CO can have psychological effects on the individuals involved, including post-traumatic stress [17]. DoD exchange programs with private companies and the employment of part-time, cyber reservists helps develop a better understanding of such effects and fosters institutional

resilience. To further reduce the burden on the defender, the strategy calls for penetration testing of internal networks to identify vulnerabilities before adversaries and introducing automated patch management. Moreover, the strategy mentions the need to deter potential threat actors through statements of policy and demonstrations of powerful intrusion detection, attribution [18], and retaliation capabilities.

3.2 China and Russia

The information warfare doctrinal approach of China and Russia differs from the US. In a 2009 paper, Timothy Thomas sets out these how these countries operate in cyberspace [19]. China's doctrine makes little reference to the 'cyber' prefix, preferring to consider computer systems and networks as a target for informationization. China's approach to informationization (and by extension CO) involves the pre-emptive use of stratagems, methods, and technology to control networks. The goal is to achieve an information advantage over the cognitive process of an adversary. The reference to pre-emptive action acknowledges the fact that CO takes time (sometimes several years) to prepare, but are required to deliver sudden, intended effect. Chinese doctrine suggests the use of CO to compromise (but not control) networks should occur in peacetime in response to strategic threat assessments. To achieve this, China must pre-emptively recruit talented individuals and establish links with the private sector. However, the Chinese military aims to avoid becoming too dependent on computer systems and information networks. The doctrine notes that Occidental (Western) armed forces rely heavily on solving problems with fragile technical solutions. A better approach, the Chinese suggest, is to focus on building cognitive resilience.

Russia also prefers to use the term informationization to describe CO. Russian doctrine on the subject states the purpose of informationization/CO as being to deliver reflexive control over an adversary. Reflexive control refers to the exploitation of weaknesses in a cognitive system to predict or influence decisions. The doctrine categorizes weakness into two types; information-technical and information-psychological. One example of information-psychological weakness might be the personal characteristics of a military commander (experience, belief, knowledge, etc.) that inform their decisions. Information-technical refers to the hardware, software, and data that facilitate and contribute to a cognitive process. Thomas cites the Russian military strategist Col. Leonenko [20] to suggest that the absence of intuition in computer cognition makes them vulnerable to reflexive control. A piece of software cannot tell, for instance, the difference between normal data and deceptive data.

Moreover, Leonenko argues that the introduction of semi- and fully autonomous systems represents a dangerous evolution in military capability. Autonomous cognition requires environments of certainty. Commanders trust these systems to make independent decisions, yet they cannot respond to previously unseen circumstances. Schneier proposes that network defense represents one area where trust in automated responses has been misplaced [21].

3.3 United Kingdom (Royal Navy)

The Cyber primer [22] forms the primary source of published UK doctrine on CO. The document provides a high-level overview of cyberspace and introduces the way the UK plans to conduct CO. In line with the layered domain model, the UK MOD approaches cyberspace as an operating environment across the physical, virtual, and cognitive domains that is formed of information networks and data. However, the definition fails to acknowledge the human component of cyberspace, on which all non-autonomous information networks depend. Terminology serves a vital role in the interpretation of doctrine. Failure to acknowledge the role of people (unlike the Russians) shall misguide commanders about the potential reach of CO.

The MOD considers CO as taking place in the near, mid, and far spaces of cyberspace. Near describes the information networks under the direct control and assurance of the Armed Forces. The mid-space exists in the networks of friendly third-parties (allies, other government departments, etc.). Those networks that are outside the control and assurance of the MOD or friendly third-parties are described as far operating spaces.

Within these spaces, the Armed Forces conduct defensive and offensive CO, alongside cyber intelligence, surveillance, and reconnaissance, and operational preparation of the environment. The UK doctrine highlights the need for the incorporation of these operations into wider military planning, to provide commanders with a 'full spectrum' targeting capability. The doctrine acknowledges the limitations of CO to affect the operational and tactical levels of conflict. Access to adversarial information networks often takes years to achieve, which means that offensive CO shall take place before any military activity, delivering an advantageous effect at the onset (e.g., Israeli bombing of Syrian reactor).

The MOD manages the resources with which to conduct CO centrally through the Joint Forces Cyber Group. Within the group sits Joint Cyber Unit (JCU) Cheltenham and JCU Corsham, deliver offensive and defensive CO capability respectively. The technically complex nature of offensive CO means that the mandate to conduct them is held at the JCU level. Nonetheless, the Royal Navy cyber strategy [23] describes the inherent advantages regarding mobility, persistence, and proximity to target that maritime platforms offer. In a sense, the Royal Navy provides a near cyberspace environment through which to conduct CO against other maritime platforms and littoral information networks. For example, warships and submarines equipped with powerful directional antennas will be able to intercept wireless internet traffic or exploit access points in coastal areas.

While JCU Corsham holds overall authority for defensive CO, the responsibility to defend specific assets exists at the single service level. The Royal Navy faces several unique challenges in this area. Naval platforms depend on a multitude of networked systems, including communication, navigation, propulsion, life-support (water, waste, etc.), and weapons. Vulnerabilities in these systems pose a significant risk to operational effectiveness.

Moreover, the technical limitations around the transfer of data over long distances means that naval platforms depend on low bandwidth communication (measured in kB/s). This causes problems for the distribution of vulnerability patches and software updates to deployed warships and submarines. The lack of bandwidth also means that the Royal Navy must employ network monitoring and active defense capabilities at the platform (local) level. Warships and submarines must respond to and recover from the initial effects of CO without external support. To address this challenge, the Royal Navy introduced Cyber Protection Teams (CPTs). Three levels of Royal Navy CPTs exist underneath JCU Corsham (Figure 1). Each platform shall deploy with at least a Level One CPT in the role of a system administrator to protect against day-to-day cyber threats [24]. Level Two CPTs shall deploy onboard larger platforms (aircraft carriers, landing ships) to provide increased protection (e.g., active network monitoring). The CDOC is the central coordinator for Royal Navy defensive CO and offers a deployable Level Three (expert) capability when required.

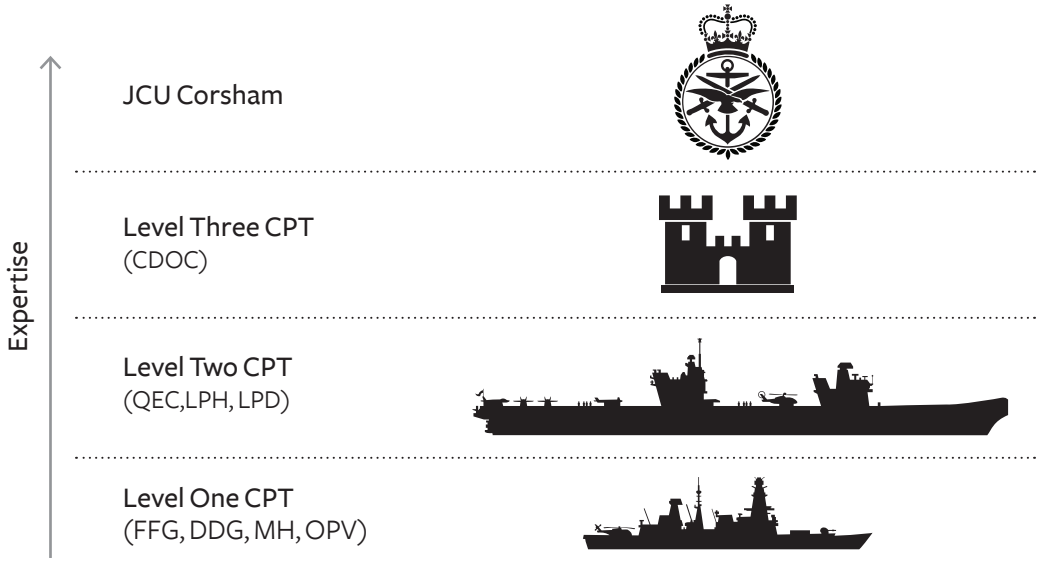

Figure 1. Hierarchy of Royal Navy Defensive CO

Members of the CDOC stress that their primary mission is to remotely track and manage vulnerabilities in the systems of deployed units. However, a significant issue faced by the CDOC is the lack of commercial openness inherent in traditional military network procurement which drives the emergence of Vendor 'lock-in' [25]. Failure to escape technological lock-in results in the use of legacy systems, with known vulnerabilities, to deliver operational capability. Moreover, contractual arrangements mean the CDOC is unable to perform penetration testing against these systems or make modifications to mitigate vulnerabilities.

4. CYBER RECRUITMENT AND TRAINING

Personnel employed in the CDOC come from the full-time trained strength of the Royal Navy's Information Warfare Division. Separate to this, the establishment of the Maritime Cyber Reserve in 2014 [26] provided the Royal Navy with a means by which to recruit talented individuals from the private sector. Moreover, the Royal Navy recruits a small proportion of civilian maritime cyber reservists who, in normal circumstances, would fail to meet the physical entry requirements. Maritime cyber reservists augment the activities of the JCUs and provide the workforce for the Royal Navy Reserve Cyber Unit. The specialist nature of the work undertaken by cyber reservists necessitates that their career advancement occurs within the confines of their respective unit and that promotion is based on merit rather than the length of service. The MOD uses an aptitude test, together with a competency framework of four levels (Awareness, Practitioner, Senior Practitioner, and Expert) to measure technical skill and to allocate cyber roles. For example, members of Level One CPTs require at least an Awareness competency. To achieve the Awareness and Practitioner competencies, individuals must attend a series of technical training courses. The role of these courses is important in developing a skill set that applies to real-world cyber-security. As Conklin et al., point out, graduates of cyber-related degree programs often lack the practical skills from real-world experience required for such activity [27].

The 'Advanced Course in Engineering (Information Assurance)' established by academics [28] at the United States Air Force Research Laboratory, provides an excellent example of an intensive, technical training program for armed forces personnel in cyber roles. The course takes place over an eleven-week period and exposes participants to a significant number of the concepts that apply to CO. Each week individuals on the course must write a thirty to forty-page report on a subject introduced by experts from across defense, academia, and industry. In parallel, the participants are divided into two teams, and each team is expected to apply the lessons they learn to conduct CO against the other. The course culminates in a large-scale East vs. West Capture the Flag (CTF) exercise, involving cyber-physical elements such as drones and rovers.

The CTF format serves as the basis for most system-on-system CO training activities. Cowan et al. provide an overview of the normal components of a CTF exercise [29]. CTF consists of at least two networked teams in competition against one another. Each team owns a server with known vulnerabilities, on which resides a data file (the flag). To score points, a team must compromise the server of an opponent and replace the flag with their own. At the same time, the team must defend their network and prevent their flag from being compromised. An independent server monitors the network and scores teams for successful offensive and defensive CO. To encourage teams to think cleverly about their actions, the score server places a fine on bandwidth usage. While not directly applicable to maritime CO (i.e., there is no attempt to achieve "reflexive control"), CTF exercises provide technical experience and help participants understand the pressures that come with CO.

5. KEY RECOMMENDATIONS

The Royal Navy should:

- Update doctrine definitions of cyberspace to recognize the human component.
- Introduce a talent-scout model of recruitment ('tap-on-the shoulder') to find individuals with exceptional skills and to create the perception of the Royal Navy as an elite place to work.
- Establish viable career paths for regular, full-time personnel who wish to work in cyber roles.
- Procure mechanisms to reduce the operational and tactical effects of CO in times of conflict (e.g., distributed software-defined networking, and virtualization).
- Ensure those employed to monitor the information networks on platforms understand how to respond and recover from CO locally.
- Work with commercial CERTs to understand the psychological risks to those who conduct high-intensity defensive CO.
- Utilize simulations and models of platform networks to train personnel involved in defensive and offensive CO. Work with the cyber-security community to introduce CTF elements into training exercises like INFORMATION WARRIOR and 'Flag Officer Sea Training'.
- Approach the introduction of autonomous and artificially intelligent systems [30] with caution, and in acknowledgement of their unsuitability to environments of uncertainty.

6. CONCLUSION

This paper illustrates many of the risks and opportunities faced by the Royal Navy in cyberspace. A diverse range of threat actors works to collect and control information by exploiting vulnerabilities that exist in the networks and systems that form cyberspace. For military organizations, the harm caused by these activities often reaches beyond the intended victim network or system, damaging operational and strategic functions. Defense doctrine serves a crucial role in communicating these dangers to planners and decision-makers to help formulate response mechanisms and mitigation strategies. The Royal Navy approach to defensive CO focuses on the need to protect platforms at the local level. CPTs deployed on board ships and submarines aim to mitigate day-to-day threats, while expert CPTs are prepared to respond to significant incidents. The US DoD strategy highlights the importance of cooperation with private sector cyber-security groups who have extensive experience in defensive CO.

Offensive CO, on the other hand, present opportunities for armed forces to augment traditional military activities. The Russian and Chinese literature on the subject discusses how informationization (offensive CO) targets the cognitive functions (autonomous and human) of an adversary to control their decisions. The Royal Navy appreciates the potential of such operations, especially when conducted by persistent and mobile maritime platforms. The service must develop understanding and experience in this area through regular CTF-type exercises.

Overall, the Royal Navy has made good progress in establishing the organizational structures and concepts with which to conduct CO. The naval service must now build the confidence to survive, operate and fight in cyberspace.

NOTES

1. D. Ormrod, and B. Turnbull, "The cyber conceptual framework for developing military doctrine", Journal of Military and Strategic Studies Volume 16, Issue 3, May 31, 2016, 270-298.

2. Development, Concepts and Doctrine Centre, "Cyber primer (second edition)", Joint Doctrine Publication, Ministry of Defence 2016, [Technical Report], https://www.gov.uk/government/publications/cyber-primer.

3. HM Government, "National security strategy and strategic defence and security review 2015: A secure and prosperous United Kingdom", November 2015. [Technical Report], https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

4. I. Driva, "Maritime Cyber Security for Navigation and Control Systems", MSc Dissertation, School of Electronics and Computer Science University of Southampton, September 2, 2016.

5. VERTIC, A. Muti, and K. Tajer, with L. Macfaul, "Cyberspace: An assessment of current threats, real consequences and potential solutions", The Remote Control Project, October 2014, [Technical Report], http://remotecontrolproject.org/publications/cyberspace-an-assessment-of-current-threats-real-consequences-and-potential-solutions/.

6. M. D. Cavelty, "Cyber-Security and threat politics: US efforts to secure the information age", Routledge, Abingdon, 2008.

7. R. Langer with G. McGraw, "An Interview with Ralph Langner", Silver Bullet Podcasts, Show 059, Cigital, February 25, 2011, https://www.cigital.com/podcasts/show-059/.

8. D. Fulghum and R. Wall, "Israel Shows Electronic Prowess: Attack on Syria shows Israel is master of the high-tech battle", Aviation Week Intelligence Network, November 26, 2007, http://aviationweek.com/awin/israel-shows-electronic-prowess.

9. M. N. Schmitt, "Tallinn manual on the international law applicable to cyber warfare", NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, Cambridge, 2013.

10. N. Perlroth, "Hackers in China Attacked The Times for Last 4 Months", NY Times, January 30, 2013, https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

11. Mandiant Intelligence Center, "Apt1: Exposing one of China's cyber espionage units.", Mandiant, 2013, [Technical Report], Available at https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

12. Permanent Select Committee on Intelligence, "(U) Review of the unauthorized disclosures of former National Security Agency contractor Edward Snowden", United States House of Representatives, September 15, 2016, [Technical Report], https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf.

13. D L. Bibighaus, "How power-laws re-write the rules of cyber warfare", Journal of Strategic Security, Volume 8, Issue 4, Henley-Putnam University, 2015, 39-52.

14 N N. Taleb, "The black swan: The impact of the highly improbable", (The Incerto Collection), Random House and Penguin, London, 2007.

15 A. Carter, "The DOD cyber strategy.", Department of Defense, Washington D C, 2015, [Technical Report], https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

16 Defense Technical Information Center, "Joint Publication 3-12(R): Cyberspace Operations", Joint Electronic Library, June 8, 2018, [Technical Report], http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

17 V. Pegueros, "DocuSign CISO Discusses The Human Element of Incident Response Security", Current Podcasts Show 105, 25 February 2011, https://traffic.libsyn.com/insight/Vanessa_Pegueros_-_Human_Element_of_IR_-_2-28-2017.mp3.

18 Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

19. T. Thomas, edited by F. Kramer, et al, "Nation-state cyber strategies: Examples from China and Russia.", Cyberpower and National Security, University of Nebraska Press, 2009, 465-488.

20. S. Leonenko, "Refleksivnoe upravlenie protivnikom [Reflexive control of the enemy]", Armeiskii sbornik (Army Collection), Issue 8, 1995, 28.

21. Schneier B, "Crypto-Gram", Schneier on Security, April 15, 2017, https://www.schneier.com/crypto-gram/archives/2017/0415.html.

NOTES

22. Development, Concepts and Doctrine Centre, "Cyber primer (second edition)", Joint Doctrine Publication Ministry of Defence, 2016, [Technical Report], https://www.gov.uk/government/publications/cyber-primer.

23. Royal Navy, "Cyber Strategy", Navy Command Headquarters, 2014.

24. RNTM 165/16, "Cyber Essentials: Level One Cyber Protection for the Naval Service", Royal Navy, 2016.

25. J. Connah, A. Solomon, J. McInnes, and O. Worthington, "Openness in military systems", Defence Science and Technology Laboratory (DSTL), 2012 Military Communications and Information Systems Conference (MCC), Gdansk, October 8-9, 2012.

26. CMRTM 24/14, "Maritime Cyber Reserves and the Formation of the RNR Cyber Unit", Commander Maritime Reserves, 2014.

27. A. Conklin, R E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the US: An analysis of the critical factors", 2014 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, January 2014, 6-9.

28. Jabbour K and Older S, "The Advanced Course in Engineering on Cyber Security: A Learning Community for Developing Cyber-Security Leaders", Syracuse University, 2004.

29. C. Cowan, S. Arnold, S. Beattie, C. Wright, and J. Viega, "Defcon capture the flag: Defending vulnerable code from intense attack.", DARPA Information Survivability Conference and Exposition, 2003 Proceedings, Volume 1, IEEE, Washington D C, April 2003, 22-24.

30. A. Johnston, "Innovation Challenge - Artificial Intelligence in Royal Navy Warships", techUK, London, October 17, 2016, https://www.techuk.org/events/briefing/item/9400-innovation-challenge-artificial-intelligence-in-royal-navy-warships.