The Current State of Research in Offensive Cyberspace Operations

Gazmend Huskaj
Department of Military Studies, Swedish Defence University, Stockholm, Sweden
gazmend.huskaj@fhs.se

Abstract: Cyber-attacks have increased since the 1988-Morris worm and can target any connected device from any place in the world. In 2010, Stuxnet received a lot of attention as the first cyber-weapon. Its targets were the Iranian nuclear enrichment centrifuges. Nation states are developing cyberspace capabilities to conduct offensive cyberspace operations. Academic researchers have been calling for a more transparent discussion on offensive capabilities and have pointed out the positive impact researchers had during the development of nuclear capabilities. Shrouded in secrecy, the development of offensive capabilities used for operations makes it difficult to conduct research. Therefore, one way to mitigate this is to conduct a systematic review of the current state of research in offensive cyberspace operations. The systematic review method makes it possible to establish certain inclusion and exclusion criteria and systematically go through academic articles to identify the contents, thoughts and research focus of academic researchers. Six scientific databases were queried and 87 articles were read and clustered. The first insight is that, based on the results of the queried databases, research about offensive cyberspace operations is limited. The resulting clusters are a general cluster about cyberspace operations, followed by research in policy, decision-making, governance, capabilities, levels, models, training, deterrence and international affairs. These are then further grouped into: a) general cyberspace operations; b) deterrence; c) international affairs; d) modelling, simulation and training. The article concludes that research into offensive cyberspace operations is maturing as more information is becoming public. Secondly, current research lists some good basic ideas regarding effects which can be achieved through offensive cyberspace operations, how they should be conducted, and related tools, techniques and procedures. However, discrepancies in research efforts exist, with the majority of research coming primarily from the western world. In addition, secrecy and the resulting limited access to information, coupled with research being either too technically focused or too qualitatively focused, show that there still remains room for research in this field. Finally, some directions for future research are examined.

Keywords: research in offensive cyberspace operations, cyberspace operations, decision-making, systematic literature review

1. Introduction

Cyber-attacks have increased since the 1988-Morris-worm (Spafford, 1988) and can target any connected device from any place in the world. Cyber-attacks are defined as actions affecting the confidentiality, integrity and availability of information in information systems. In 2010, Stuxnet was dubbed as the first cyber-weapon, targeting Iranian nuclear enrichment centrifuges (Stark, 2011). “Targeting is the process of selecting and prioritizing targets” (Joint Chiefs of Staff, 2018, p.IV-8). Nation states are developing capabilities to conduct offensive cyber operations. Researchers have been calling for a more transparent discussion on offensive capabilities, pointing out the positive impact researchers had during the development of nuclear capabilities.

The motivation for this article is twofold; firstly, to give readers a description of the current state of research in offensive operations. Secondly, to show where this research is focused. In this article, cyberspace is defined as internetworked information systems. Peterson and Davie (2012) define internetworked as ‘the concept of interconnecting different types of networks to build a large, global network.’ Valacich and Schneider (2010), and Laudon and Traver (2011) have defined information systems (the reader is advised to those authors for the full definitions). Therefore, the long definition of internetworked information systems (i.e. cyberspace) is “hardware and software which are used to create, process, store, retrieve and disseminate information in different types of interconnected networks that build a large, global network, built and used by people.” This definition is grounded and tangible, and there is no better place to provide it than in a literature review. The scope of the article is defined by the inclusion and exclusion criteria.

This article is organised around two research questions:

- (RQ1) What is the current state of research in offensive cyber operations?
- (RQ2) Where is that research focused?

This work contributes to PhD-students who want to explore the topic and decide on a research direction. It also contributes to active researchers and practitioners who want to get insights on the current thoughts and ideas in the area.

The first section describes the method. The second section presents the results followed by discussion and conclusions.

2. Method

Major contributions to scientific research are found on databases (Webster and Watson, 2002). The search used the search query "offensive cyber operations." Searching terms enclosed in quotation marks causes search engines to only present articles containing those exact phrases (Blachman & Peek, 2012). The initial search results were:

Source	Description and Implementation	Results
IEEE Xplore	The database "is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity." The database holds 4,338,558 items at the time of writing.	Four
ScienceDirect	The database is "Elsevier's leading platform of peer-reviewed scholarly literature" and holds "over 14 million peer-reviewed publications."	14
Scopus	The database is "the largest abstract and citation database of peer-reviewed literature."	19
SpringerLink	The database holds "over 10 million scientific documents." Of these, only 15 were accessible by the author. One of the articles was in German.	54
Web of Science	The database is "your ideal single research destination to explore the citation universe across subjects and around the world."	9
WorldCat	The database is "the world's largest library catalog."	80

Firstly, articles were screened based on their titles and abstracts. Permutations of the articles were removed. The remaining articles were skimmed through their titles and abstracts to evaluate their relevance and quality based on the inclusion and exclusion criteria. The inclusion criteria were published articles, books or chapters in books, conference papers or MSc-theses. The exclusion criteria were articles published prior to year 2000 and non-English articles. Only one article was non-English and is unlikely to skew the results. Next, they were clustered manually into the following research areas:

- General cluster about cyberspace operations
- Policy
- Decision-making
- Governance
- Capabilities
- Levels
- Models
- Training
- Deterrence, and
- International Studies

The author established a review form covering the main argument, key concepts/assumptions, results and cluster/category, and a free text field for major points to make in the discussion. The review form was constructed iteratively.

3. Results

This section presents the results of the reviewed articles and some quantitative measures in Table 1. It should be noted that the categorisations are not mutually exclusive, e.g. some articles cover multiple research fields. In addition, even though not all of the 87 articles reviewed are cited below, a reasonably representative sample of articles is included in each category.

Table 1: Characteristics of the 87 articles. Note that the categorizations used are not mutually exclusive

General Cyber Operations	49
Deterrence	16
International Affairs	10
Governance	2

Policy	13
Decision-making	5
Capabilities	9
Levels	7
Models & Simulation	7
Training	4

3.1 General overview of offensive operations

This category covers the broader topics regarding offensive operations, followed by targets, vulnerabilities, tactics, techniques and procedures, and proxies.

Eilstrup-Sangiovanni (2017) describes how governments are investing in offensive capabilities: at least 29 governments have dedicated units, and at least 60 more are developing capabilities. Douglass (2012) and Bardin (2015) note which countries are developing offensive capabilities and Kshetri (2016) highlights North Korean offensive operations. Harrison & Herr (2016), Jajodia et al. (2016) and Ottis (2015) note that state and non-state actors, intelligence agencies and military organisations conduct offensive operations. Gompert and Binnendijk (2016) note that offensive operations have certain characteristics making them favourable compared to conventional forces, while Sutton (2013) and Torres (2012) describe the effects of offensive operations in the Georgia 2008-case. Dossi (2018) discusses that offensive operations are conducted through proxies, increasing the difficulty of attribution. Fernandes et al. (2018) and Bardin (2015) discuss US and Israeli investments, while Yeo et al. (2015) and Fernandes et al. (2013) discuss how the US Department of Defense (DoD) has increased the transparency of their capability. Buchanan (2017) compares levels of maturity between countries, and Lin (2010) describes a process for operations. Iasiello (2013) notes how China and Iran use offensive operations to monitor, censor and block information from reaching the public. Finally, Rochetto (2016) notes that terrorist groups lack the skills, tools, resources and determination to conduct offensive operations. Resources include encryption, exploits and staff (Sin et al., 2016).

This category describes targets. Caire (2018) discusses attacking critical infrastructure and transportation systems to bind or deny an adversary's resources. Hart and Klink (2017) argue that offensive operations can enable information operations, while Van der Velt (2017) argues that the Russians weaponised information to affect trust in the US elections. Kallberg and Thuraisingham (2013) identify information systems, networks, infrastructure and industries as possible targets, while their military counterparts are off-limits. Ormrod (2014) also argues for targeting command, control, communications, computers and intelligence, surveillance, and reconnaissance (C4ISR) networks. Porche, et al. (2017) argues for targeting unmanned aerial systems (UAS), adversary units and their devices in a mission area. Uren (2017), Nevill (2016) and Hawkins (2016) disclose that Daesh has been targeted by Australian offensive operations.

This category discusses the use of vulnerabilities for offensive operations. Sigholm and Larsson (2014) discuss exploiting the "Heartbleed Bug" for an offensive operation, while Charlet et al. (2017), Schwartz and Knake (2016) discuss the importance of the Vulnerability Equities Process (VEP), a policy on vulnerabilities. The VEP balances the national security interests of collecting intelligence from foreign nations and terrorist groups, and securing the infrastructure against threats (Schwartz & Knake, 2016). Charlet et al. (2017) note that the government notify software vendor(s) to create a patch once a vulnerability is used for national security purposes.

This category covers tactics, techniques and procedures (TTPs) for offensive operations. Eriksson and Pettersson (2017) compare offensive operations with special operations: small scale, requiring high secrecy and high operator skills, and with high political risk. Grant (2013) notes similarities with special operations in that they operate under government authority and comply with national and international law. Hurley (2017) argues that the nation state, as well as the private and public sectors, can conduct offensive operations. Offensive operations serve to defeat or destroy an enemy, while in the private sector they can "increase shareholder value and market share" (p.19).

This category discusses the use of proxies for offensive operations. Kallberg and Rowlen (2014) note that countries with low cyber-maturity are at risk of being used as proxies. This tactic decreases the risk of attribution to the attacking country but increases the risk for the proxy-nation. Bardin (2015) notes Iran using proxies such

as Hamas and Hezbollah. Borghard and Lonergan (2016) note how Russia used proxies in the 2008-Georgia-case. Forums were used to coordinate attacks targeting Georgian high-value targets. The use of proxies can also reduce costs because offensive capabilities require significant skills to develop and maintain access. In addition, it is easier to provide proxies with computers than weapons.

3.2 Deterrence

This category discusses how offensive operations can increase a nation's deterrence posture. Fischerkeller (2017) notes that offensive operations can generate physical damage, influence adversarial actions, collect intelligence and be integrated into conventional operations to achieve new effects. Eilstrup-Sangiovanni (2017), Lonsdale (2017), and Mazanec (2015) note that a strong offensive capability can achieve enhanced credibility for strategic deterrence.

3.3 International affairs

This category discusses the role of law. Lin (2017) argues that decision-makers will have a more comprehensive understanding of offensive operations if legislation requires military organisations to report to the government on these activities. Smyth (2014) states that offensive operations should adhere to the Law of Armed Conflict. Prescott (2012) cites the DoD policy whereby offensive operations are conducted in the same way as their kinetic capabilities, adhering to "policy principles and legal regimes, including the Law of Armed Conflict" (p.261). Cusumano and Corbe (2018) note that some nations employ illegal and inappropriate means, and misuse international law.

3.4 Governance

Governance constitutes a small part of the literature. Douglass (2012) and Rodriguez (2011) discuss governance at government level and at operational/tactical level. Governance in the US is currently spread across a confusing myriad of competing authorities, crippling the capacity to operate offensively in cyberspace. Rodriguez (2011) argues that offensive operations at operational/tactical level fall within the area of responsibility of the geographic combatant commander.

3.5 Policy

Research on policy in support of offensive operations is limited. A policy on offensive operations assists decision-makers, supports national interests and makes it possible to pursue political goals (Baltrusaits, 2017; Olagbemiro, 2014; Nikitakos & Mavropoulos, 2014). A policy can also clarify any potential future confrontation between nation states (Segal, 2016). It is difficult to promote norms, deter attacks and pursue political goals without a policy. (Johnson, 2014; Nikitakos and Mavropoulos, 2014). Buchanan (2017) discusses the positive impact of U.S. Presidential Policy Directive 20, including how it directs the community to plan, prepare and present cases where offensive operations may be used.

3.6 Decision-making

In decision-making, Grant (2017), Prescott (2013) and Oltramari et al. (2013) discuss how to speed up decision-making processes. This is important due to the speed of cyber-attacks. Another option is to have automated decision-making processes (ADPs) assisting human decision-makers (Prescott, 2013; Oltramari et al, 2013). However, ADPs must have the principles of the Law of Armed Conflict and rules of engagement "incorporated into ADP design processes" (Prescott, 2013, p.3). Finally, Grant (2017) and Uren (2017) discuss the organisation of the offensive capability with related decision-making processes.

3.7 Capabilities

Capabilities are required to achieve desired effects. Buchanan (2017) argues that cyber operations should be conducted early for the development of offensive capabilities. They may be used for operations in preparation of the environment and exploiting system vulnerabilities. This requires intelligence, surveillance and reconnaissance capabilities (Harrison and Herr, 2016). Capabilities in hostile networks should be covert, which Jajodia et al (2016) discuss. McArdle (2016) agues the Chinese and Russians prefer "soft" capabilities because of the level of deniability. Soft capabilities are those just below the threshold of triggering armed responses.

3.8 Strategic and tactical levels operations

This category presents research on levels of operations. Rõigas (2018), Lin and Zegart (2017), Lemieux (2015), Andress and Winterfield (cited by Lemieux, 2015), and Cartin (cited by Wilson and Drumhiller, 2015) discuss the strategic level of offensive operations. Lemieux (2015) states they are aligned with defensive and offensive operations; Andress and Winterfield (2015) argue defensive operations are within the dimensions of prevention and deterrence. Cartin (2015) argues the goal is to "influence the perception of one's security" (p.34). Lin and Zegart (2017) state their focus should be on the long term, while Rõigas (2018) notes the strategic role of offensive operations is still unclear. On the tactical level, Lin and Zegart (2017) state offensive operations are focused on a small area with short-term goals, while Lemieux (2015) notes tactical operations as "techniques and practices to secure or penetrate a computer network" (p.2).

3.9 Modelling and simulation

Models can be effective tools to conduct offensive operations. Buchanan (2017) presents an eight-step model while Grant (2012) presents a five-step model. Rochetto (2016) compares a nation state adversary with an adversary group, noting that the group cannot put the same efforts into stealth due to a lack of skills and resources.

3.10 Training

Training, education and certain traits are essential to the conduct of offensive operations. Aybar (2017) describes developing a virtual environment mimicking an adversary's system to train personnel before deployment. Burke and van Heerden (2016) present a cyber challenge, rigged with sensors, to train operational behaviour. Schweizer et al. (2013) have a course for students on offensive operations. De Souza (2013) discusses certain traits, which personnel designated for offensive and defensive operations should have.

4. Discussion

The current state of offensive cyber operations indicates further opportunities for research. This section discusses some observations while answering the research questions.

4.1 General cyber operations

Governments are conducting offensive operations. Researchers have listed (in alphabetical order) China, Iran, Israel, North Korea, Russia, and the US as countries conducting offensive operations and increasingly investing in that capability. The researchers highlight the importance of capabilities to achieve desired effects, but none of them discusses the fact that capabilities are developed through software development cycles to exploit vulnerabilities in target systems. Ethical dilemmas regarding whether or not to release vulnerabilities exist. The literature highlights how the vulnerability equities process is a solution which has two positive effects. Firstly, it communicates a level of maturity on the authorities conducting offensive operations; secondly, it increases the level of trust between the private and public sectors. The private sector know they will receive information from the government when software flaws are identified. The intelligence services collect information about vulnerabilities in target systems, which may be used as a list of requirements to develop the capability. Developing capabilities may take time. This could be one variable to take into account when deciding whether the operation is at a strategic or tactical level. However, researchers disagree as to what strategic offensive operations are. There may be two reasons; firstly, cyber operations are not fully understood because their possibilities will be revealed as more devices become connected; secondly, because of the nature of offensive operations, as already mentioned above. However, regardless of level, tactics, techniques and procedures for offensive operations require more research. Current research on TTPs is focused mostly on comparing offensive operations with special operations. While this may be true, research explaining and describing TTPs for offensive operations is lacking, especially in the technical-policy area, i.e. describing the impact of technology on policy without using too technology-oriented language. Finally, the decision on whether to hit the target directly or go through proxies needs to be considered. Until now, the use of proxies has been an accepted way to conduct operations, and those most at risk are the countries used as proxies. Therefore, one interesting question is, what areas are off-limits for use as proxies?

4.2 Deterrence

Offensive operations increase a nation's deterrence posture. To do this, offensive operations need to be credible and communicated through the media. Credibility is achieved by conducting operations and "leaking", i.e. releasing information in a controlled fashion, to the media. Intelligence can also be revealed jointly with allies. This may include information on the adversary, their targets, the indicators of compromise, and advice on how to patch any vulnerabilities the adversary has been exploiting.

4.3 International affairs

Decision-makers have a hard time to grasp the abstract world of cyberspace and the affiliated political risk connected with offensive operations. Political risk is mitigated by adhering to international law, the Law of Armed Conflict, and the same policy principles as for kinetic capabilities. To make it tangible, offensive operations may be compared to Special Forces operations.

4.4 Policy, decision-making and governance

The lack of research on policy in offensive operations makes it difficult for decision-makers to know who does what at national level. The only known model for policy in support of operations is PPD20, and is US-specific. A policy in support of offensive operations will likely increase cooperation between competing agencies. In addition, it is likely to have positive effects on deterrence; the level of uncertainty with which the country conducts retaliatory-operations is increased and would-be attackers may be deterred. In addition, it may also increase the speed of decision-making processes. These are required for retaliatory actions. Another way is to use automated decision-making processes for retaliatory actions. However, risks exist. Is the source really the target who attacked or was it a proxy? What are the risks of cascading effects? Will an automatic response lead to escalation? Could an adversary have tampered with the algorithms responsible for automated-decision-making processes? These are some of the issues that have to be considered. Finally, governance is important for effective offensive operations. Governance spread across competing authorities cripples the effectiveness of offensive operations and affects credibility of deterrence. Governance at the operational/tactical level is equally important, if not more so, to achieve the desired effects on adversary targets.

4.5 Modelling, simulation and training

Modelling, simulation and training are important tools to plan, prepare and train for offensive operations. The results show that models differ on the number and order of steps. It may well be so that there is no single model for offensive operations based on context and resources. Training for offensive operations requires virtual environments and courses. However, only one researcher discusses the importance of personality traits for offensive and defensive operations. This area requires more research in order to mitigate the risk of insider threats to the operational security of offensive operations.

5. Conclusions and future work

This article has presented a review of the scientific literature on offensive cyber operations. Six scientific databases were queried, resulting in 180 articles. Of these, 87 articles were reviewed after screening. It is evident that some research describes actors investing, developing and conducting offensive operations. In contrast, less research is focused on governance, training and decision-making. Furthermore, there is an opportunity for research in processes for operations: Lin (2010) describes one. The answer to (RQ1) what is the current state of research in offensive cyber operations is covered by 4.1-4.5. The answer to (RQ2) where research is focused is depicted by Table 1. It is evident that a lot of research is focused on general offensive operations, deterrence and policy. However, there is room for more research on governance, training and decision-making. Overall, there is potential for more research, especially in processes for operations.

Acknowledgements

The author would like to thank Johan Sigholm, PhD, for his valuable inputs to the manuscript.

References

Baltrusaits, D. F. (2017). Cyber warfare Cyber War: Do We Have the Right Mindset? In *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense* (pp. 1–22). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-06091-0_24-1

Bardin, J. (2015). Cyber Operations in the Middle East. In F. Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice* (pp. 97–110). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137455550_7

Blachman, N., and Peek, J. Quotation Marks Replace the + Operator. Retrieved from http://www.googleguide.com/quote_operator.html.

Borghard, E. D., & Lonergan, S. W. (2016). Can States Calculate the Risks of Using Cyber Proxies? *Orbis*, *60*(3), 395–416. https://doi.org/10.1016/j.orbis.2016.05.009

Brantly, A. F. (2016). The decision to attack: military and intelligence cyber decision-making. *The Decision To Attack: Military and Intelligence Cyber Decision-Making*.

Brantly, A. F. (2016). The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace. *SAIS Review of International Affairs*, *36*(2), 29–39. https://doi.org/10.1353/sais.2016.0018

Buchanan, B. (2017). *The Intruder's View*. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Vol. 1). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.003.0003

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 557–562. https://doi.org/10.1109/PERCOMW.2017.7917623

Burke, I., & Van Heerden, R. P. (2016). Automating cyber offensive operations for cyber challenges. *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016*, (Marczewski 2013), 65–73.

Charlet, K., Romanosky, S., & Thompson, B. (2017). It's Time for the International Community to Get Serious about Vulnerability Equities, *0*.

Colloquium, B., & Bruges, C. De. (2010). Technological Challenges for the Humanitarian Legal Framework. *Bruges Colloquium*, (October).

Eriksson, G., & Petterson, U. (2017). *Special Operations from a Small State Perspective*. (G. Eriksson & U. Pettersson, Eds.). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-43961-7

Fischerkeller, M. (2017). Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies. *Survival*, *59*(1), 103–134. https://doi.org/10.1080/00396338.2017.1282679

Flahive, M. P. (2015). *Breaking Bad: Reforming Cyber Acquisition Via Innovative Strategies*. Air Command and Staff College Air University.

Gompert, D., & Binnendijk, H. (2016). The Power to Coerce: Countering Adversaries Without Going to War. https://doi.org/10.7249/RR1000

Grant, T. (2015). Specifying functional requirements for simulating professional offensive cyber operations. *Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS 2015*, (March), 108–117.

Grant, T. (2017). Grant, T.J. (2017). Speeding up Parliamentary Decision Making for Cyber Counter-Attack. In Bryant, A.R., Lopez, J.R. & Mills, R.F. (eds.), Proceedings, 12, (March), 152–159.

Grant, T. J. (2013). Tools and Technologies for Professional Offensive Cyber Operations. *International Journal of Cyber Warfare and Terrorism*, *3*(3), 49–71. https://doi.org/10.4018/ijcwt.2013070104

Grant, T., Burke, I., & van Heerden, R. (2012). Comparing Models of Offensive Cyber Operations. *International Conference on Information Warfare and Security*, (January), 108–121.

Grant, T., Eijk, E. van, & Venter, H. (2016). Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time. *11th International Conference on Cyber Warfare and Security: ICCWS2016*, (March), 146.

Hart, S. W., & Klink, M. C. (2017). 1st Troll Battalion: Influencing military and strategic operations through cyber-personas. In *2017 International Conference on Cyber Conflict (CyCon U.S.)* (pp. 97–104). IEEE. https://doi.org/10.1109/CYCONUS.2017.8167503

Hawkins, Z. (2016). Digital land power: the Australian Army' s cyber future, 2016–2018. Retrieved from https://www.aspistrategist.org.au/digital-land-power-australian-armys-cyber-future/

Heickero, R. (2015). Russia's Information Warfare Capabilities. In *Current and Emerging Trends in Cyber Operations* (pp. 65–83). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137455550_5

Herr, T., & Herrick, D. (2016). Understanding Military Cyber Operations. In R. M. Harrison & T. Herr (Eds.), *Cyber Insecurity* (p. 412). Rowman & Littlefield Publishers.

Howard, D. (2014). Virtue in Cyberconflict. In L. Floridi & M. Taddeo (Eds.) (Vol. 14, pp. 155–168). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-04135-3_10

Hurley, J. S. (2017). Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense. https://doi.org/10.1007/978-3-319-06091-0

Irion, K. (2013). *The Secure Information Society*. (J. Krüger, B. Nickolay, & S. Gaycken, Eds.), *The Secure Information Society: Ethical, Legal and Political Challenges*. London: Springer London. https://doi.org/10.1007/978-1-4471-4763-3

Jajodia, S., Subrahmanian, V. S., Swarup, V., & Wang, C. (2016). Cyber deception: Building the scientific foundation. *Cyber Deception: Building the Scientific Foundation*, 1–312. https://doi.org/10.1007/978-3-319-32699-3

Johnson, M. C. (2014). *Refining United States Policy on Offensive Cyber Operations*. Air University.

Joint Chiefs of Staff. (2018). Joint Publication 3-12: Cyberspace Operations.

Josang, A. (2014). Potential Cyber Warfare Capabilities of Major Technology Vendors. *Proceedings of the 13th European Conference on Cyber Warfare and Security (Eccws-2014)*, (July), 110–115.

Kallberg, J., & Cook, T. S. (2017). The Unfitness of Traditional Military Thinking in Cyber: Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*, *5*, 8126–8130. https://doi.org/10.1109/ACCESS.2017.2693260

Kallberg, J., & Rowlen, S. (2014). African nations as proxies in covert cyber operations. *African Security Review*, *23*(3), 307–311. https://doi.org/10.1080/10246029.2014.924976

Kallberg, J., & Thuraisingham, B. (2013). *Chapter 19 – From Cyber Terrorism to State Actors' Covert Cyber Operations*. *Strategic Intelligence Management*. https://doi.org/10.1016/B978-0-12-407191-9.00019-3

Kshetri, N. (2016). Cybersecurity in South Korea. In *The Quest to Cyber Superiority* (Vol. 2010, pp. 171–182). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-40554-4_10

Kshetri, N. (2016). The Quest to Cyber Superiority. https://doi.org/10.1007/978-3-319-40554-4

Land, C. A., & Centre, W. (n.d.). *For Canada's future army*.

Lee, J.-A. (2015). The Sino-US Digital Relationship and International Cyber Security. In *Current and Emerging Trends in Cyber Operations* (pp. 84–96). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137455550_6

Lehto, M. (2015). Cyber Security: Analytics, Technology and Automation, *78*, 3–29. https://doi.org/10.1007/978-3-319-18302-2

Lemieux, F. (2015). Trends in Cyber Operations: An Introduction. In F. Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*. Palgrave Macmillan.

Lin, H. (2017). Cybersecurity and Deterrence - A Notification Requirement for Using Cyber Weapons or for Unauthorized Disclosure of a Cyber Weapon.

Lonsdale, D. J. (2017). Warfighting for Cyber Deterrence: a Strategic and Moral Imperative. *Philosophy & Technology*. https://doi.org/10.1007/s13347-017-0252-8

McArdle, J. (2016). An Assessment of Russian and Chinese Offensive Cyber Operations on U.S. Space Assets. In E. Sterner & J. McArdle (Eds.) (pp. 10–22).

Nevill, L. (2016). Cyber wrap. Retrieved from https://www.aspistrategist.org.au/cyber-wrap-145/

Nikitakos, N., & Mavropoulos, P. (2014). Cyberspace as a State's Element of Power. In *Cyber-Development, Cyber-Democracy and Cyber-Defense* (Vol. 9781493910, pp. 259–277). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4939-1028-1_10

Olagbemiro, A. O. (2014). Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyber Warfare. United States Army Command and General Staff College Fort Leavenworth, Kansas.

Oltramari, A., Lebiere, C., Vizenor, L., Zhu, W., & Dipert, R. (2013). Towards a cognitive system for decision support in cyber operations. *CEUR Workshop Proceedings*, *1097*, 94–100.

Ormrod, D. G. A. (2014). A "wicked problem" - Predicting sos behaviour in tactical land combat with compromised C4ISR. *Proceedings of the 9th International Conference on System of Systems Engineering: The Socio-Technical Perspective, SoSE 2014*, 107–112. https://doi.org/10.1109/SYSOSE.2014.6892472

Ottis, R. (2015). Cyber Security: Analytics, Technology and Automation, *78*, 89–96. https://doi.org/10.1007/978-3-319-18302-2

Prescott, J. M. (2012). Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States ? *2012 4th International Conference on Cyber Conflicts*, *8*(May 2011), 251–266.

Schwartz, A., & Knake, R. (2016). Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process. *Harvard Kennedy School - Belfer Center*, *3*, 28.

Schweitzer, D., Gibson, D., Bibighaus, D., & Boleng, J. (2013). Preparing our undergraduates to enter a cyber world. *IFIP Advances in Information and Communication Technology*, *406*, 123–130. https://doi.org/10.1007/978-3-642-39377-8_13

Segal, A. (2016). U.S. Offensive Cyber Operations in a China-U.S. Military Confrontation. *SSRN Electronic Journal*, (March 2016). https://doi.org/10.2139/ssrn.2836203

Sidari, B. D. (2016). *Offensive Cyber Operations: The Need for a Policy to Contend with the Future*.

Sigholm, J., & Larsson, E. (2014). Determining the utility of cyber vulnerability implantation: The heartbleed bug as a cyber operation. *Proceedings - IEEE Military Communications Conference MILCOM*, 110–116. https://doi.org/10.1109/MILCOM.2014.25

Sin, S. S., Blackerby, L. A., Asiamah, E., & Washburn, R. (2016). Determining extremist organisations' likelihood of conducting cyber-attacks. *International Conference on Cyber Conflict, CYCON*, *2016–August*, 81–98. https://doi.org/10.1109/CYCON.2016.7529428

Smyth, V. (2014). The Best Defense is a Good Offense: Conducting Offensive Cyberoperations and the Law.

Spafford, E. (1988). The Internet Worm Program: An Analysis. Retrieved from https://spaf.cerias.purdue.edu/tech-reps/823.pdf.

Sprengers, M., & van Haaster, J. (2016). *Organization of #operations*. *Cyber Guerilla*. https://doi.org/10.1016/B978-0-12-805197-9.00003-6

Stark, H. (2011). Mossad's Miracle Weapon - Stuxnet Virus Opens New Era of Cyber War. Der Spiegel.

Subrahmanian, V. S., Mannes, A., Sliva, A., Shakarian, J., & Dickerson, J. P. (2013). Policy Options Against LeT. In *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba* (pp. 157–176). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4614-4769-6_11

Sutton, W. S. (2013). Cyber Operations and the Warfighting Functions, 32.

Torres, A. M. (2012). Offensive Cyber is Fires, A Case for MAGTF Integration, *3330*(703).

Witte, J. C. (2015). *The Panacea and the Square Peg: Strategic Fallacies of the Air, Undersea and Cyber Domains*.

Yeo, S., Birch, A. S., & Bengtsson, H. I. J. (n.d.). The Role of State Actors in Cybersecurity (pp. 217–246). https://doi.org/10.4018/978-1-4666-9661-7.ch013.