2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)

Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks

Max Smeets
Department of Politics and International Relations
University of Oxford
Oxford, UK
max.smeets@politics.ox.ac.uk

Abstract: Organisational Integration has become a key agenda point for policy-makers as governments continue to change and create new organisations to address the cyber threat. Passing references on this topic, however, far outnumber systematic treatments. The aim of this paper is to investigate the potential effects of organisational integration of offensive cyber capabilities (OIOCC). I argue that OIOCC may lead to three key benefits: enhanced interaction efficiency, greater knowledge transfer and improved resource allocation. There are, however, several negative effects of integration, which have so far received little attention. OIOCC may lead to an intensification of the cyber security dilemma, increase costs overall, and impel 'cyber mission creep'. Though the benefits seem to outweigh the risks, I note that ignoring the potential negative effects may be dangerous, as activity is more likely to go beyond the foreign-policy goals of governments and intrusions are more likely to trigger a disproportionate response by the defender.

Keywords: *organisational integration, offensive cyber capabilities, cyber weapons*

1. INTRODUCTION

The principle of organisation integration (OI) is commonly examined in relation to firms' performance.[1] OI is perceived to be a form of organisational innovation, with its potential value on a par with technological innovation.[2] It is considered to be an essential means for firms to remain competitive in the market. Governments often seek OI too, as a way to reduce costs or provide services more effectively. Extending Kenneth Waltz's famous analogy between the market economy and the international state system, one might even say that integration helps states to enhance their relative power in the international system and ensure survival.[3]

OI is also a key agenda point for senior policy-makers seeking to find effective ways to address the cyber threat.[4] The institutional landscape has been shaken up by the new cyber security challenges that countries face. South Korea, for example, has a National Cybersecurity Centre which leads investigations into cyber security incidents. It also has a National Cyber Threat Joint Response Team, comprised of actors from the military, civilian and private sectors, which provides assistance during a crisis. South Korea's CERT manages cyber incidents (there is also a private CERT called CONCERT). And within the Ministry of National Defence it has established a Cyber Command.[5] Similarly, the Netherlands has established various organisations like the National Cyber Security Centre, the Cyber Security Council, the Defence Cyber Education and Training Centre, and the Defence Cyber Command.[6] It has also expanded the missions of several organisations including the National Coordinator for Counter Terrorism and Security, and the Ministry of Security and Justice.

In most countries, the creation and reorientation of institutions dealing with cyber security is ongoing and occurs in parallel to a range of other initiatives such as strategy formulation, regulation, and the creation of informal partnerships. To 'defend the core' effectively requires

1 It occupies a central place in several bodies of literature, including organisational theory, management, information systems, and organisational strategy. Jay Barney, 'Firm resources and sustained competitive advantage', *Journal of Management*, 17:1 (1991), 99-120; Ricardo Chalmeta, Christina Campos, Reyes Grangel, 'Reference architectures for enterprise integration', *The Journal of Systems Software*, 57 (2001)175-191; John Ettlie and Ernesto M. Reza, "Organizational Integration and Process Innovation', *Academy of Management Journal*, 35:4 (2001), 795-827; Gregory E. Truman, 'Integration in electronic exchange environments', *Journal of Management Information Systems*, 17:1 (2000), 209-244.

2 Ettlie and Reza, 'Organizational Integration and Process Innovation'.

3 Kenneth Waltz, *A Theory of International Politics*, (New York: McGraw-Hill: 1979).

4 See, for example, the most recent national cyber security strategy of the United Kingdom: 'UK Government, National Cyber Security Strategy 2016-2021', (2016). Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf; or Australia: Chris Brookes, 'Cyber Security: Time for an integrated whole-of-nation approach in Australia', Centre for Defense and Strategic Studies, (March 2015). Retrieved from: http://www.defence.gov.au/ADC/Publications/IndoPac/150327%20Brookes%20IPS%20paper%20-%20cyber%20(PDF%20final).pdf.

5 This is not an inclusive list of institutions. For an overview, see: International Telecommunication Union, 'Cyberwellness Profile Republic of Korea', (December 1, 2014). Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Korea.pdf; James Andrew Lewis, 'Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States', Inter-American Development Bank, Discussion Paper IDB-DP-457, (2016, July). Retrieved from: https://publications.iadb.org/bitstream/handle/11319/7759/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United%20States.pdf?sequence=.

6 National Cyber Security Centrum, 'Cybersecuritybeeld Nederland CSBN 2016', (2016); The Netherlands Ministry of Justice, 'De Nationale Cybersecurity Strategie 2: Van bewust naar bekwaam', (2013, October); The Netherlands Ministry of Defence, 'Cyber Command'. Retrieved from: https://www.defensie.nl/english/topics/cyber-security/contents/cyber-command.

awareness about how these organisations and activities can be balanced, coordinated and combined. In other words, it requires an understanding of OI in relation to cyber security.

However, passing references far outnumber systematic treatments of this issue. We know that organisational design and internal politics play a central role in the use of military capabilities, yet organisational analysis is a comparatively underdeveloped aspect of the study of the use of cyber capabilities. Scholars who set out to explain the use of cyber capabilities normally arrive at arguments that focus on the 'nature' or 'meaning' of cyberspace. Yet we cannot fully understand the use of cyber capabilities without studying the organisational structure in which its use of these capabilities is embedded. Through this analysis, we acknowledge that organisational structure can potentially shape the use of offensive cyber capabilities.

I therefore seek to address the following question: *what are the potential effects of organisational integration of offensive cyber capabilities (OIOCC)?* I argue that OIOCC may lead to three key benefits: enhanced interaction efficiency, greater knowledge transfer, and improved resource allocation. There are however several negative effects of integration, which have so far received little attention. OIOCC may lead to an intensification of the cyber security dilemma,[7] increase costs overall, and impel 'cyber mission creep'. Though the benefits seem to outweigh the risks, I note that ignoring the potential negative effects may be dangerous, as actors are more inclined to go beyond the foreign-policy goals of governments and intrusions are more likely to trigger a disproportionate response by the defender.

OI in relation to cyber security occurs at different levels and for different purposes. Table 1 provides a basic overview of the different types of OI. First, the table distinguishes between defensive and offensive organisational activities. Second, it distinguishes between three levels of integration: the highest level refers to the integration of cyber activities between the government and other entities such as the private sector; mid-level OI refers to integration between government organisations of which some do not (initially) focus on cyber activities; and the lowest level considers organisational integration between organisations which focus on cyber activities.[8]

The aim of this paper is to investigate the lowest level of OI in relation to the development of offensive cyber capabilities. According to NATO's Deputy Assistant Secretary General for Emerging Security Challenges, Jamie Shea, 'about 100 countries in the world – 100 countries, which is the majority – are actively developing offensive, not defensive, but offensive – cyber capabilities'.[9] Similar estimates are provided in a report from James Lewis written for the United Nations, and others provide more conservative estimates.[10]

7 See section 4 for an explanation of this dilemma.

8 Notice that the categories found in the table concern 'ideal types' of OI which serve to clarify the scope of this paper. In practice, these forms of OI probably overlap.

9 Jamie Shea, 'Lecture 6 - Cyber attacks: hype or an increasing headache for open societies?', (29 February, 2012). Retrieved from: http://www.nato.int/cps/en/natolive/opinions_84768.htm; For a similar statement see: INFOSEC, 'The Rise of Cyber Weapons and Relative Impact on Cyberspace', (October 5, 2012). Retrieved from: http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/.

10 James Lewis, 'The Cyber Index: International Security Trends and Realities', United Nations Institute for Disarmament Research, 2013. Retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf; Kim Zetter, 'We are at Cyberwar: A global guide to nation-state digital attacks', *Wired*, 2015. Retrieved from: https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/.

TABLE 1. TYPES OF OI IN RELATION TO CYBER SECURITY

		Defence	Offence
High-Level OI	Government organisation – Proxy, Private, or other State	Type A[11]	Type D[12]
Mid-Level OI	Government organisation with no cyber activities – Government organisation with cyber activities	Type B[13]	Type E[14]
Low-Level OI	Government organisation with cyber activities – Government organisation with cyber activities	Type C[15]	Type F[16]

I focus on this level because it is the one which has received the least amount of rigorous analysis but where the stakes are potentially the highest. Unlike discussions about initiatives promoting defensive measures, offensive cyber capability development has remained shrouded in secrecy, perhaps even more so than conventional security issues. Yet organisational mismanagement of offensive cyber activity can lead to unnecessary cycles of provocation, with potentially disastrous consequences.[17]

OIOCC is not only relevant for those states which seek to establish initial operability to conduct sophisticated cyber attacks. In fact, OIOCC also addresses some of the core concerns that

11 Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', *Information & Security*, 7, (2001), 80-103; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age* (Routledge: 2008); Robert K. Knake, 'Internet Governance in an Age of Cyber Insecurity', Council on Foreign Relations, Special Report No.56, (2010); Jerry Brito and Tate Watkins, 'The Cybersecurity-Industrial Complex', *Reason*, 43,4 (2011); Myriam Dunn-Cavelty, and Manuel Suter, 'Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection', *International Journal for Infrastructure Protection*, 2(2009), 179- 187; Shmuel Even, 'The Strategy for Integrating the Private Sector in National Cyber Defense in Israel', *Military and Strategic Affairs*, 7:2 (2015).

12 See Tim Maurer, '"Proxies" and Cyberspace', *Journal of Conflict and Security Law*, 21:3 (2016) 383-403; Tim Maurer, 'Cyber Proxies and the Crisis in Ukraine', in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (NATO CCD COE Publications: Tallinn: 2015); Richard Clarke, 'War from Cyberspace', *National Interest*, 104 (2009), 31-36.

13 Rachel Yould, 'Beyond the American Fortress: Understanding Homeland Security in the Information Age'. In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. (The New Press: 2003); John Tritak, 'Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems?', Hearing before the Committee on Energy and Commerce, (5 April 2001).

14 Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (Simon & Schuster: New York: 2016); The US Department of Defense, 'The DoD Cyber Strategy', (April 2015); Sorin Ducaru, 'The Cyber Dimension of Modern Hybrid Warfare and its relevance for NATO', *Europolity*, Continuity and Change in European Governance, 10:1 (2016). Retrieved from: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf; Frank Hoffman, 'Hybrid Warfare and Challenges', *Joint Force Quarterly*, 52 (2009), 34-39.

15 Cheryl Pellerin, 'New Threat Center to Integrate Cyber Intelligence', US Department of Defense, (February 11, 2015). Retrieved from: https://www.defense.gov/News/Article/Article/604093; Richard Bejtich, 'What are the Prospects for the Cyber Threat Intelligence Integration Center?' Brookings Institution, (February 19, 2015). Retrieved from: https://www.brookings.edu/blog/techtank/2015/02/19/what-are-the-prospects-for-the-cyber-threat-intelligence-integration-center/.

16 Mark Pomerleau, 'Services integrating cyber and traditional military forces', (September 30, 2016). Retrieved from: http://www.c4isrnet.com/articles/services-integrating-cyber-and-traditional-military-forces.

17 For example, it can lead to the use of offensive capabilities not in line with legal conduct or increase the chances of 'cyber accidents'.

highly advanced cyber powers are currently grappling with. Adam Segal penned five takeaways from the annual 'National Thought Leaders' visit to the National Security Agency (NSA) in December 2016: i) the reasoning for 'loud' cyber weapons;[18] ii) the splitting of NSA and Cyber Command;[19] iii) the need for a new workforce model; iv) private sector outreach; and v) the creation of a new cyber force.[20] Through this OI analysis, in which I also analyse how the development of offensive cyber capabilities is distinctive compared to other processes, we gain a better understanding of how some of these critical challenges can be resolved.

The remainder of this paper is structured as follows. First, it deals with the first-order question of defining OI and OIOCC. It also discusses the optimal product design of offensive cyber capabilities and current forms of OIOCC. In the second part, I develop several propositions about the general benefits of OIOCC. The third part develops three propositions about the potential negative effects of integration, and the final part concludes and draws out lessons on which form of OI would be suitable for the development of offensive cyber capabilities.

2. THE NATURE OF OI AND OIOCC

There are dozens of definitions of organisational integration. For the purposes of this discussion, I follow Lawrence and Lorsch's definition of OI as 'the process of achieving unity of effort among the various subsystems in the accomplishment of the organisation's tasks'.[21] In more poetic terms, integration is about achieving and committing to a harmonious marriage of activities. Like any good marriage, there are many ways in which OI can be successfully achieved.[22]

As a primary step to understanding the nature and requirements of OIOCC, a discussion of the desired 'output' is required. The expectation is that OIOCC of states is directed towards the development of *sophisticated* capabilities.[23] Sophistication in this context refers to the complexity of techniques put into the development of a capability to enable it to gain

18 As Segal writes 'A senior official confirmed that sometimes Cyber Command wants an adversary to know it has conducted an operation and so in some instances it embeds the equivalent of ['from US Cyber Command' in the code'. Adam Segal, 'Takeaways From a Trip to the National Security Agency', *Council on Foreign Relations*, (December 21, 2016). Retrieved from: http://blogs.cfr.org/cyber/2016/12/21/takeaways-from-a-trip-to-the-national-security-agency/.

19 It was officially announced in December 2016 that the US will change the dual hat arrangement at the NSA and Cyber Command. See: Ellen Nakashima, 'Obama moves to split cyberwarfare command from the NSA', *Washington Post*, (December 23, 2016). Retrieved from: https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html?utm_term=.8dba21add7e9; US Department of Defense, 'Joint Concept on Cyberspace – US Department of Defense', (2011).

20 Note that, according to Segal, an official of the NSA was against the creation of a new cyber force. Segal, 'Takeaways from a Trip to the National Security Agency'.

21 Paul R. Lawrence and Jay W. Lorsch, 'Differentiation and Integration in Complex Organisations', *Administrative Science Quarterly*, 12:1 (1967), 1-47; also see Henri Barki and Alain Pinsonneault, 'A model of Organizational Integration, Implementation Effort, and Performance', *Organization Science*, 16:2 (2005)165-179; As the definition indicates, I focus on the cross-function orientation reflecting linkages *within* government, i.e. internal integration.

22 For a contrasting view, see Tolstoy's Anna Karenina Principle.

23 Note that a sophisticated actor does not always have to use sophisticated capabilities. For a more extensive discussion on this topic see: Ben Buchanan, 'The Legend of Sophistication in Cyber Operations', Harvard Kennedy School Belfer Center, Working Paper Series, (January, 2017), 1-27.

its objective.[24] As David Aitel notes, cyber operations can differ in the sourcing and use of capabilities, networking, testing, persistence and operational security.[25] This means there are no strict necessary and sufficient conditions when a capability can be considered 'sophisticated', but they share 'family resemblances' such as: i) the exploitation of zero-day vulnerabilities; ii) the implementation of various obfuscation techniques; iii) the ability to deliver payload to difficult-to-reach targets; and iv) the implementation of customised malware of firmware.[26]

Sophisticated cyber attacks generally take place across multiple stages,[27] creating a sequential interdependence between the activities.[28] We can distinguish between four general stages.[29] The first stage is *reconnaissance*. This includes the attacker 'sniffing' (to eavesdrop on existing data traffic), 'footprinting' (to gain knowledge of the network or security posture), and 'enumeration' (to identify user accounts which can potentially be exploited). The second stage concerns intrusion. We commonly distinguish between user intrusion (with non-administrative user privileges) and root intrusion (with administrative user privileges). The third stage of a cyber attack is *privilege escalation*.[30] At this stage a vulnerability is exploited in an operating system (OS) or specific service or software package. Finally, there is the stage which gives away the *goal* of the attacker. This could be denial of service (DoS), installation of a backdoor, exfiltrating data, espionage or corruption (with as its aim to cause harm or damage). The order of activities conducted by Advanced Persistent Threat (APTs) is often highly complex, and different tasks may be executed – even outside cyberspace – with long periods of time in between. For example, a backdoor (i.e. a way to bypass normal authentication) may be initially installed at t=0, and check-ups might take place in later time periods t=1, t=2, and t=3 to see if it still exists, but a future attack using that backdoor might occur only in t=x.

The optimal product design of a sophisticated offensive cyber capability – which OIOCC aims to help achieve – meets four criteria. First, it should be *effective* in achieving its desired goal. In the case of a cyber weapon, this means it can reliably provide unauthorised access to a computer system to cause harm or damage to a living being or system.[31] Second, it needs to comply with

24 See Max Smeets, 'What it Takes to Develop a Cyber Weapon', Columbia University SIPA: Tech & Policy Initiative, Working Paper Series 1 (2016), 49-67.

25 David Aitel, 'Useful Fundamental Metrics for Cyber Power', *CyberSecPolitics*, 2016. Retrieved from: https://cybersecpolitics.blogspot.com/2016/06/useful-fundamental-metrics-for-cyber.html.

26 Ibid. I differ from Aitel, as his framework does not distinguish between type of vulnerability exploited (i.e. zero-day versus non-zero-day exploits).

27 The term 'multi-stage attack' is often used in the literature. However, it has two different meanings. For Landau and Clarke this occurs when computer A penetrates computer B, which is then used to penetrate computer C, and so on. For others (see for example Rid and Buchanan), multi-stage is when a cyber attack occurs through steps that can be temporarily be distinguished. I refer to the latter meaning in this article. See David D. Clarke and Susan Landau, 'The problem isn't attribution; it's multi-stage attacks', *ACM ReArch*, (November 30, 2010); Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38:1-2 (2015), 4-37.

28 Other common forms of interdependence concern 'pooled interdependence' and 'reciprocal interdepended'. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory*, (McGraw-Hill: 1967).

29 I follow the framework of: S. Mathew, R. Giomundo, S. Upadyaya, M. Sudit, and A. Stotz, 'Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams,' VizSEC '06, Proceedings of the 3rd International Workshop on Visualization for Computer Security (2016)1-6; Other frameworks exist, see for example: FireEye, 'Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks', WhitePaper, (2012). Retrieved from: http://www.softbox.co.uk/pub/fireeye-advanced-targeted-attacks.pdf.

30 This is usually for buffer overflow attacks, in which the program overwrites memory adjacent to a buffer that should not have been modified.

31 Smeets, 'What it Takes to Develop a Cyber Weapon'.

(international) legal standards. A responsible actor seeks more from a weapon than merely the ability to cause harm or damage. Principally, the weapon needs to be discriminate, in that it can be used in accordance with the principles of distinction and proportionality.[32] Third, the development should be *cost efficient* in that it produces the desired result for the least amount of resources poured into it. Finally, it needs to be at an actor's disposal on a permanent basis. For industries, a key factor leading to OI is the demand for steady volumes of output or the assurance that a service is available at all times.[33] In the context of offensive cyber capability development, ideally, governments aim to organise their operations in such a manner that the 'cyber option' is always available as a potential (strategic) asset to use.

One should also be aware of what OIOCC does *not* aim to achieve. A key goal of OI is normally to standardise the output of a process, especially in the manufacturing industry. The aim of a manufacturer is to ensure that every final product has the same properties. For example, customers drinking a certain soda brand expect that their drink will have the same taste each time they buy it. Yet, as Lindsay and Gartzke observe, the essential element of cyber weapons' success is deception, with its basic tactics of dissimulation (hiding what is there) and simulation (showing what it is not).[34] As the attacker constantly needs to find innovative ways to mislead the enemy to ensure the attack is successful, uniform products are *not* desired.[35]

As we can observe from the activities of various governments, OIOCC can come in many shapes and forms: through appointing the same director for the intelligence services as for the command conducting military activities; through establishing a significant intelligence constituency within the military command; through offering the same training programme to those conducting espionage operations and those conducting offensive (destructive) cyber operations; and through people moving from an intelligence gathering unit to a military unit and vice versa. There is no ideal configuration of integration, as it depends on size and capital (also human capital) of the cyber operations. There are however a number of potential benefits and risks of OIOCC which are discussed below.

3. THE BENEFITS OF OIOCC

I develop three propositions about the positive effects of OIOCC in helping to achieve 'optimal' output: i) interaction efficiency, ii) knowledge transfer and organisational learning and iii) mission overlap.

A. Proposition 1: OIOCC Leads to Interaction Efficiency of Intelligence and Military Activities

The obstacles that actors have to overcome to conduct a sophisticated cyber attack are often

32 Legal compliance increases the costs of development due to the additional need for testing, grading costs, and the losses of rejected capabilities.

33 J.A. Seagraves and C.E. Bishop, 'Impacts of Vertical Integration on Output and Industry Structure', *Journal of Farm Economics*, 40 (1968), 1814-1827.

34 Lindsay and Gartzke consider deception to be a distinct strategy, similar to deterrence in the nuclear era. Erik Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies*, 24:2, (2015), 316-348.

35 As Martin Libicki states, there is no 'forced entry' when it comes to offensive cyber operations. Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 31-36.

underestimated.[36] Smeets distinguishes between three different types of obstacles for different types of capabilities: first, there are the knowledge/intelligence barriers to overcome in developing a capability; second, there are economic and material obstacles; and third, there are organisational obstacles as various actors have to work together to develop a certain capability.[37] With respect to the latter, the interdependence between the intelligence collection activity and the military activity is essential as a great amount of preparation is required to understand the targeted systems.[38] OI facilitates this interaction, making it the most obvious benefit.

The importance of this close link between intelligence and military has been well-documented in the case of Stuxnet.[39] As Jon Lindsay observes:

> Stuxnet infections have been traced to five different industrial companies within Iran, all of which dealt in [Industrial Control System] equipment […]. These domains were infected on multiple occasions with an average of nineteen days between malware compilation and the date of infection.[40]

To match Stuxnet's payload with the specific type of programmable logic controller required highly specific intelligence, and to engineer a 'perfect' code, thorough testing was required. A mock-up plant was therefore created using Qaddafi's P-1 centrifuges.[41] Over time, the tests grew in size and sophistication. According to David Sanger, at some point the United States and Israel were 'even testing the malware against mock-ups of the next generation of centrifuges the Iranians were expected to deploy, called IR-2s, and successor models, including some the Iranians still are struggling to construct'.[42] Overall, as Lindsay concludes, 'the Stuxnet operation required substantial time and institutional infrastructure'.[43] Like the small elements of a high-quality Swiss clockwork beautifully working together to show the time with complete precision, to conduct a sophisticated cyber operation like Stuxnet, a close connection between numerous actors and processes is necessary.[44]

36 Smeets, 'What it Takes to Develop a Cyber Weapon'; Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22:3 (2013), 365-404.

37 Smeets, 'What it Takes to Develop a Cyber Weapon'.

38 This means a serial relationship exists as the output from the reconnaissance operation becomes the input for the cyber operations with as aim to cause harm or damage.

39 Stuxnet was allegedly developed and deployed by the United States and Israel. The origins of the worm go back as early as 2006, midway through George W. Bush's second term, as the administration aimed to diversify its options against Iran. David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Random House: New York: 2012).

40 Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22:3 (2013), 365-404.

41 Ibid.

42 Sanger, 'Confront and Conceal', 198.

43 Lindsay, 'Stuxnet and the Limits of Cyber Warfare', 387.

44 According to Rob Morgus, there was potentially a similar close link in Russia's cyber operations against Ukraine. Also Kim Zetter writes that 'skilled and stealthy strategists [launched] a synchronized assault in a well-choreographed dance.' Yet, considering that there were clear delineations between the various phases of the operations suggests that this was a form of collaboration (between potentially criminal and nation-state actors, as Zetter writes) rather than integration. Robert Morgus, 'Whodunnit? Russia and Coercion through Cyberspace', 2016. Retrieved from: https://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/; Kim Zetter, 'Inside the Cunning Unprecedented Hack of Ukraine's Power Grid', *Wired*, 2016. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

B. Proposition 2: OIOCC Increases the Opportunity for Knowledge Transfer

OIOCC also stimulates the transfer of knowledge. Knowledge transfer refers to the process through which one individual, group, or unit is affected by the experience of another.[45] Empirical evidence suggests that interconnected organisations such as franchises and alliances hold comparative advantages over their more autonomous counterparts due to the ability to transfer knowledge across their constituent parts. For example, a restaurant may put a new dish on the menu that was successfully served at its sister restaurant located in a different part of town.[46]

The required knowledge component for developing offensive cyber capabilities comes in two forms.[47] First, there is the part which is explicit and can be transferred in a systematic manner. For example, it concerns knowledge about how different elements of an industrial control system work. Another example of this form of knowledge is the ability of a person to write code in a certain programming language. The most significant knowledge component is often tacit and difficult to articulate.[48] For example, this might concern knowledge embedded in a hacker's experience or a cyber command's implicit operational processes.[49] The tacit knowledge required to conduct offensive cyber activities cannot be formally communicated. Forms of OIOCC, however, allow for the opportunity to also transfer this type of knowledge.

C. Proposition 3: OIOCC Minimises Mission Overlap and Improves Resource Allocation

Finally, OIOCC allows for a more efficient allocation of resources, because the same processes or tasks are not replicated unnecessarily. In any organisation, some overlap in tasks is inevitable; yet OIOCC leads to enhancement resource allocation on three levels.

First, it can put people to better use. In a number of countries, the growth of offensive cyber capabilities in militaries already allowed for greater specialisation in cyber weapon production. The US Cyber Command now has 133 teams in operation, making it easier to dedicate specialised units to specific types of cyber operations.[50] OI frees up further resources for specialisation. This means that task complexity can be increased, as tasks can be divided on the basis of who is most proficient in the process. Second, 'capital' can be used more efficiently. Two basic forms of 'capital' of offensive cyber capabilities concern software and infrastructure. On the former, software can often be divided into smaller modules (called modularity); OIOCC makes it easier to reuse parts of code from a different operation in order to save time and resources. On the latter, a type of infrastructure frequently used by attackers is command and control (C&C) servers, which help to maintain communications with compromised machines. Also, to launch

45 Linda Argote, Paul Ingram, John M. Levine, and Richard L. Moreland, 'Introduction: Knowledge Transfer in Organizations: Learning from the Experience of Others', *Organizational Behavior and Human Decision Processes*, 82 (1) (2000), 1-8; 3.

46 Ibid, 4.

47 Smeets, 'What it Takes to Develop a Cyber Weapon'.

48 Michael Polanyi, *Personal Knowledge: Towards a Post-Critical Philosophy*, (University of Chicago Press, Chicago: 1958).

49 See also: Thomas Rid, *Cyber War Will Not Take Place*, (C. Hurst & Co: London: 2013), 83-84; Martin Davies, 'Knowledge – Explicit, implicit and tacit: Philosophical aspects', in *International Encyclopaedia of Social and Behavioral Sciences*, James D. Wright (ed.) (Elsevier: 2015).

50 According to Rob Morgus, this was also the case for Russia's cyber operations against Ukraine. Robert Morgus, 'Whodunnit? Russia and Coercion through Cyberspace', *War on the Rocks*, 2016. Retrieved from: https://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/.

distributed denial-of-service (DDoS) attacks, a botnet of 'zombies' (compromised computers) are often used flood the bandwidth of a targeted system.[51] Again, integration makes it easier to repurpose this type of infrastructure for a different cyber operation.[52] Third, and related, OIOCC makes it easier to leverage previous activities and accomplishments. For example, if a backdoor in a computer system is already established by one actor, it can conveniently be used by another.

4. THE RISKS OF OIOCC

Organisational integration, however, does not only have positive consequences. I consider three propositions about the negative effects created by OIOCC.

A. Proposition 1: OIOCC Intensifies the Cyber Security Dilemma

A prominent theoretical idea in International Relations is the security dilemma. The situation occurs in an anarchical system when states cannot be certain about each other's intentions. Mutual fear leads states to resort to an accumulation of capabilities to defend themselves, which in turn leads to (unintended) spirals of worsening relationships with a potentially tragic outcome.[53] Buchanan indicates that also a cyber security dilemma exists, as states which aim to assure their own (cyber) security have an incentive to intrude into strategically important networks of other states and will thus threaten – often unintentionally – the security of those other states, risking escalation.[54]

The first potential downside of OIOCC is that it intensifies this cyber security dilemma. The knowledge transfer incentive, mentioned above as a positive effect of OIOCC, also has a negative externality for the development of offensive capabilities. Argote and Ingram note that '[k]nowledge transfer in organisations manifests itself through changes in the knowledge or performance of the recipient units'.[55] It leads to a loss of distinct organisational cultures with their practices and 'playbooks'. The commonality in behaviour of OIOCC further blurs the line between when a cyber espionage operation ends, and a destructive operation starts. From the

51 See Rid and Buchanan, 'Attributing Cyber Attacks', 17.

52 FireEye offers an example in their report on attribution of advanced cyber attacks: 'four separate attacks that use different exploits, different lures, and different first-stage malware implants. But they all target religious activities. And […] they are all sent from the same server […]. This evidence points to multiple actors on the same team, using the same infrastructure'. See: FireEye, 'Digital Bread Crumbs: Seven Clues to Identifying Who's Behind Advanced Cyber Attacks', (2013, June). Retrieved from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-digital-bread-crumbs.pdf.

53 For original formulations, see: Herbert Butterfield, *History and Human Relations*, (London: Collins, 1951); John Herz, *Political Realism and Political Idealism: A Study in Theories and Realities*, (Chicago: University of Chicago Press, 1951); Robert Jervis, *Perception and Misperception in International Politics*, (Princeton, NJ: Princeton University Press, 1976), Chap. 3; and Jervis, 'Cooperation under the Security Dilemma', *World Politics* 30: 2 (1978), 167–214. For a more recent review see: Shiping Tang, 'The Security Dilemma: A Conceptual Analysis', *Security Studies*, 18:3 (2009), 587-623.

54 For a more detailed discussion see: Ben Buchanan, *The Cyber Security Dilemma*, (Oxford: Oxford University Press: 2017).

55 Linda Argote and Paul Ingram, 'Knowledge Transfer: A Basis for Competitive Advantage in Firms' *Organizational Behavior and Human Decision Processes*, 82:1 (2000), 150-169.

defenders' viewpoint, it is more difficult to discern the cyber attackers' intention and accurately respond.[56]

The matter can be put into perspective considering the following (ever more relevant) question: what do we do if we find out about cyber espionage activities on our computer systems? 'Respond proportionately' would be the diplomatic answer. Indeed, in the last press conference of 2015, President Obama said the US would take 'proportionate' action in response to a cyber attack on Sony Pictures by North Korea. Proportionality was also the cornerstone of President Obama's response to the Democratic National Committee (DNC) hack. For a long time, it was unclear what the US government does against Russia's aggression, other than 'respond in a proportionate manner'.

But what does 'proportionate' mean in this context? The response is likely not just tailored towards the *actual* 'observed' activity (i.e. an espionage operation) but also the perceived *intent* of the attacker (i.e. an assessment of whether a destructive cyber attack will follow or not). The underlying rationale of the attacker is, however, difficult to interpret, especially if an espionage operation and a destructive operation are conducted in the same operational fashion. This means that we are unable to discern if our *perceived* proportionate response is *actually* proportionate or not.

B. Proposition 2: OIOCC Leads to Cost Ineffectiveness in the Long Run

Offensive cyber capability integration may seem to be economical in the short-term, but will most likely increase costs down the road. Offensive cyber capabilities are said to be transitory in nature, meaning they are relatively short lived in their ability to cause harm or damage.[57] Cyber capabilities are not equally transitory, and one of the factors which explains this differentiation concerns the type of payload. All other things being equal, it can be said that destructive cyber capabilities causing visible damage are more likely to be discovered than espionage capabilities, and hence lead to the patching of a vulnerability.[58]

However, due to the integration of activities, the deployment of a destructive cyber weapon also increases the risk that espionage capabilities – exploiting the same vulnerabilities and same coding procedures – are exposed as well. The issue is particularly pertinent now that threat intelligence firms (and possibly states) are establishing special detection tools in attempt to uncover clusters of capabilities. This means that integration makes an attacker's offensive cyber 'arsenal' more volatile and costly, as multi-year cyber programs are more susceptible to a low return on investment after capabilities with a destructive payload are used.

A more general risk stems from changes in information access due to OIOCC which may also ultimately increase costs. Integration aims to simulate knowledge transfer within the

56 The US Cyber Command has recently proposed the development of 'loud' cyber weapons for when you want to be attributed; though this raises a great number of operational questions; Chris Bing, 'US Cyber Command director: We want 'loud', offensive cyber tools', *Fedscoop*, (August 30, 2016). Retrieved from: http://fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016; Herb Lin, Developing 'Loud' Cyber Weapons (September 1, 2016). Retrieved from: https://www.lawfareblog.com/developing-loud-cyber-weapons; Herb Lin, 'Still More on Loud Cyber Weapons', *Lawfare*, (October 19, 2016) retrieved from: https://www.lawfareblog.com/still-more-loud-cyber-weapons.

57 Notice that certain cyber capabilities are more transitory than others. For a more extensive discussion on this point, see: Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyber Weapons', *Journal of Strategic Studies*, (2017), 1-28.

58 Ibid.

organization. Yet, it is inherently more demanding to manage the risks of information security (normally shortened to InfoSec) when more people are able to view classified documents and are briefed about certain operations.[59]

C. Proposition 3: OIOCC Leads to Cyber Mission Creep

Mission creep refers to the gradual expansion of a project or mission beyond its original goals. This usually occurs following the initial successes of an operation. As Caraccilo writes, 'mission creep is usually considered undesirable due to the dangerous path of each success breeding more ambitious attempts, only stopping when a final, often catastrophic, failure occurs'.[60]

The ongoing transfer of civilian tasks to military agencies has been well-documented in the case of the global war on terrorism. In 2008, US Secretary of Defense Robert Gates warned:

> [o]verall, even outside Iraq and Afghanistan, the United States military has become more involved in a range of activities that in the past were perceived to be the exclusive province of civilian agencies and organisations. This has led to concern among many organisations about what's seen as a creeping 'militarisation' of some aspects of America's foreign policy. This is not entirely unreasonable sentiment.[61]

Mission creep is also observed in domestic and international organisations.[62] Monahan, for example, critiques the emergence of data-sharing 'fusion centres' intended to reduce crime and prevent terrorism. His main critique is that:

> these centres […] mutate into 'all-crimes' and 'all-hazards' organisations […] in order to ensure their continued existence in the face of future budget cuts.[63]

It can be said that OIOCC enhances the risk of what I label cyber mission creep: the risk that an organisation responsible for offensive cyber activities goes beyond their core mission in the use of these capabilities. Cyber mission creep can come in two forms. First, there is the risk that initial intelligence activities through cyberspace go beyond their core mission and lead to the use of cyber weapons.[64] This is especially likely to occur when intelligence services in a country are perceived to be more capable than the military. The second form of cyber mission creep occurs when the military is gradually conducting more cyber activities, even when it

59 InfoSec normally has three components: i) confidentiality, ii) integrity, and iii) availability.

60 Dominic Joseph Caraccilo, *Beyond Guns and Steel: A War Termination Strategy*, (Santa Barbara: Praeger Security International), 178.

61 Robert M. Gates, 'Secretary of Defense Speech', US Global Leadership Campaign, July, 8 2008, Washington, DC; Gordon Adams and Shoon Murray, *Mission Creep: The militarization of US Foreign Policy*, (Georgetown University Press: Washington, DC: 2014).

62 Jessica Einhorn, 'The World Bank's Mission Creep', *Foreign Affairs*, 80:5 (2001), 22–35; Ngaire Woods, *The Globalizers: The IMF, the World Bank and their Borrowers* (Ithaca, NY: Cornell University Press, 2006).

63 Torin Monahan, 'The murky world of Fusion Centres', *Criminal Justice Matters*, 75:1 (2009), 20-21.

64 Although I refer to this as a new form of mission creep, I do not argue that the same dynamics which cause military mission creep cause cyber mission creep.

concerns minor (domestic) disorders rather than war or another emergency situation.[65] Indeed, there is the risk that intelligence agencies mutate into 'all-cyber' organisations.

5. CONCLUSION

In response to cyber security challenges, governments have established a wide range of informal and formal institutions. The focus of this paper was to enhance our understanding of the organisational integration of offensive cyber capabilities. In doing so, it will help states which already have developed, as well as those which are developing, offensive cyber capabilities to make better decisions about their organisational structures.

OIOCC can come in many shapes and forms, and the ideal configuration depends on a state's set up. This paper has developed in total six general propositions about the potential consequences of OIOCC. Following the propositions of the benefits of OIOCC, it was argued that integration reduces mission overlap, increases cost effectiveness, and improves communication. I also call attention to the risks of OIOCC, which are still not well understood. OIOCC deepens the cyber security dilemma and leads to potential cyber mission creep. Also, the potential cost effectiveness created through OIOCC in the short run might turn into cost ineffectiveness overall, as 'clusters' of capabilities are more likely to be discovered. Although the benefits seem to outweigh the risks, a misunderstanding of the risks can have significant consequences for conflict escalation.

This paper also presents some limitations and opportunities for future research. First, this paper has been primarily theoretical and should still be subject to empirical scrutiny in order to test the validity of the OIOCC propositions. Ideally, a comparative analysis would be conducted between countries with different levels of OIOCC to verify whether the propositions presented in this paper hold in practice. Second, it was noted that the nature of cyber capabilities places greater emphasis on innovation than on forced control. This means that in the case of OIOCC, an increase in organisational efficiency should not come at the cost of organisational and individual flexibility. More research should be conducted on the mechanisms to achieve these

65 Another form of creepism can be observed for offensive cyber capabilities, which is called in product design terms 'feature creep' (and for computer programs 'software bloat'). This refers to ongoing addition of new features in products, resulting in over-complication. We have this also with offensive cyber capabilities. Stuxnet is again a good example. Ralph Langner indicates that Stuxnet actually refers to two weapons, instead of one. While the early version focused on loosening the isolation valves of the Natanz uranium enrichment facility, the later version sought to change the speeds of the rotors in the centrifuges. Langner notes in his report that 'The attack routines for the overpressure attack [of the second version] were still contained in the payload, but no longer executed – a fact that must be viewed as deficient OPSEC. It provided us by far the best forensic evidence for identifying Stuxnet's target, and without the new, easy-to-spot variant the earlier predecessor may never have been discovered. That also means that the most aggressive cyber-physical attack tactics would still be unknown to the public – unavailable for use in copycat attacks, and unusable as a deterrent display of cyber power'. We however have not information to conclude whether this type of feature creep – leading to a less stealthy (a potentially less effective) capability – was the result of an *inter-agency* problem or an *organisational integration* problem. See: Ralph Langner, 'Stuxnet's Secret Twin', Foreign Policy, (19 November 2013). Retrieved from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/; Ralph Langner, 'To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve', *The Langner Group*, (November 2013). Retrieved from: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, 5; Geoff McDonald, Liam O Murchu, Stephen Doherty, Eric Chien, 'Stuxnet 0.5: The Missing Link' *Symantec*, (26 February, 2013). Retrieved from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.p.

goals concurrently. Third, I have limited the scope of my research to government actors; so-called 'supplier integration' of other actors has not been the focus of my research. An obvious extension would be to look at the interaction between private actors and government actors in developing offensive cyber capabilities. After all, when the demand for offensive capabilities increases (both in complexity and size), states can expand their activities by persuading legislators to increase budgets and size of departments or by taking on 'private suppliers'.

ACKNOWLEDGMENTS

For written comments on early drafts, I am indebted to Florian Egloff, Richard Harknett, Lennart Maschmeyer, Nikolas Ott, Henry Rõigas, James Shires, and anonymous reviewers. An earlier version of this paper was presented at the Oxford Cyber Studies Working Group.

REFERENCES

Adams, Gordon and Shoon Murray, Mission Creep: *The militarization of US Foreign Policy*, (Georgetown University Press: Washington, DC, 2014).

Aitel, David, 'Useful Fundamental Metrics for Cyber Power,' *CyberSecPolitics*, 2016. Retrieved from: https://cybersecpolitics.blogspot.com/2016/06/useful-fundamental-metrics-for-cyber.html.

Argote, Linda and Paul Ingram, 'Knowledge Transfer: A Basis for Competitive Advantage in Firms,' *Organizational Behavior and Human Decision Processes*, 82:1 (2000), 150-169.

Argote, Linda, Paul Ingram, John M. Levine, and Richard L. Moreland, 'Introduction: Knowledge Transfer in Organizations: Learning from the Experience of Others,' *Organizational Behavior and Human Decision Processes*, 82 (1) (2000), 1-8.

Barki, Henri and Alain Pinsonneault, 'A model of Organizational Integration, Implementation Effort, and Performance,' *Organization Science*, 16:2 (2005), 165-179.

Barney, Jay, 'Firm resources and sustained competitive advantage,' *Journal of Management*, 17:1 (1991), 99-120.

Bejtich, Richard, 'What are the Prospects for the Cyber Threat Intelligence Integration Center', Brookings Institution, (February 19, 2015). Retrieved from: https://www.brookings.edu/blog/techtank/2015/02/19/what-are-the-prospects-for-the-cyber-threat-intelligence-integration-center/.

Bendrath, Ralf, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection,' *Information & Security*, 7, (2001), 80-103.

Bing, Chris, 'US Cyber Command director: We want "loud," offensive tools,' *FedScoop* (August 30, 2016). Retrieved from: http://fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016.

Brito, Jerry and Tate Watkins, 'The Cybersecurity-Industrial Complex,' *Reason*, 43, 4 (2011).

Brookes, Chris, 'Cyber Security: Time for an integrated whole-of-nation approach in Australia,' Centre for Defence and Strategic Studies, (March 2015). Retrieved from: http://www.defence.gov.au/ADC/Publications/IndoPac/150327%20Brookes%20IPS%20paper%20-%20cyber%20(PDF%20final).pdf

Buchanan, Ben, *The Cyber Security Dilemma*, (Oxford: Oxford University Press: 2017).

Buchanan, Ben, 'The Legend of Sophistication in Cyber Operations,' Harvard Kennedy School Belfer Center, Working Paper Series, (January, 2017), 1-27.

Butterfield, Herbert, *History and Human Relations*, (London: Collins, 1951).

Chalmeta, Ricardo, Christina Campos, Reyes Grangel, 'Reference architectures for enterprise integration,' *The Journal of Systems Software*, 57 (2001), 175-191.

Clarke, David D. and Susan Landau, 'The problem isn't attribution; it's multi-stage attacks,' *ACM ReArch*, (November 30, 2010).

Clarke, Richard, 'War from Cyberspace,' *National Interest*, 104 (2009), 31-36.

Davies, Martin, 'Knowledge – Explicit, implicit and tacit: Philosophical aspects,' in *International Encyclopaedia of Social and Behavioral Sciences*, James D. Wright (ed.) (Elsevier, 2015).

Ducaru, Sorin, 'The Cyber Dimension of Modern Hybrid Warfare and its relevance for NATO,' *Europolity*, Continuity and Change in European Governance, 10:1 (2016). Retrieved from: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf.

Dunn Cavelty, Myriam and Manuel Suter, 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection,' *International Journal for Infrastructure Protection,* 2 (2009), 179-187.

Dunn Cavelty, Myriam, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age,* (Routledge: 2008).

Dominic Joseph Caraccilo, *Beyond Guns and Steel: A War Termination Strategy*, (Santa Barbara: Praeger Security International).

Ettlie, John and Ernesto M. Reza, 'Organizational Integration and Process Innovation,' *Academy of Management Journal*, 35:4 (2001), 795-827.

Einhorn, Jessica, 'The World Bank's Mission Creep,' *Foreign Affairs*, 80:5 (2001), 22-35.

Even, Shmuel, 'The Strategy for Integrating the Private Sector in National Cyber Defense in Israel,' *Military and Strategic Affairs*, 7:2 (2015).

FireEye, 'Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks,' WhitePaper, (2012). Retrieved from: http://www.softbox.co.uk/pub/fireeye-advanced-targeted-attacks.pdf.

Gartzke, Erik and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,' *Security Studies*, 24:2, (2015), 316-348.

Gates, Robert M., 'Secretary of Defense Speech,' US Global Leadership Campaign, Washington, DC (July 8, 2008).

Herz, John, P*olitical Realism and Political Idealism: A Study in Theories and Realities*, (Chicago: University of Chicago Press, 1951).

Hoffman, Frank, 'Hybrid Warfare and Challenges,' *Joint Force Quarterly*, 52 (2009), 34-39.

INFOSEC, 'The Rise of Cyber Weapons and Relative Impact on Cyberspace,' (October 5, 2012). Retrieved from: http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/.

International Telecommunication Union, 'Cyberwellness Profile Republic of Korea,' (December 1, 2014). Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Korea.pdf.

Jervis, Robert, 'Cooperation under the Security Dilemma,' *World Politics* 30: 2 (1978), 167-214.

Jervis, Robert, *Perception and Misperception in International Politics*, (Princeton, NJ: Princeton University Press, 1976).

Kaplan, Fred, *Dark Territory: The Secret History of Cyber War*, (Simon & Schuster: New York: 2016).

Knake, Robert K., 'Internet Governance in an Age of Cyber Insecurity,' *Council on Foreign Relations*, Special Report No.56, (2010).

Langner, Ralph, 'Stuxnet's Secret Twin,' *Foreign Policy*, (November 19 2013). Retrieved from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

Langner, Ralph, 'To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve,' *The Langner Group*, (November 2013). Retrieved from: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Lawrence, Paul R. and Jay W. Lorsch, 'Differentiation and Integration in Complex Organizations,' *Administrative Science Quarterly*, 12:1 (1967), 1-47.

Lewis, James Andrew, 'Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States,' Inter-American Development Bank, Discussion Paper IDB-DP-457, (2016, July). Retrieved from: https://publications.iadb.org/bitstream/handle/11319/7759/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United%20States.pdf?sequence=.

Lewis, James Andrew, 'The Cyber Index: International Security Trends and Realities,' United Nations Institute for Disarmament Research, (2013). Retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

Libicki, Martin, *Conquest in Cyberspace: National Security and Information Warfare,* (New York: Cambridge University Press, 2007).

Lin, Herb, 'Developing 'Loud' Cyber Weapons,' *Lawfare*, (September 1, 2016). Retrieved from: https://lawfareblog.com/developing-loud-cyber-weapons.

Lin, Herb, 'Still More on Loud Cyber Weapons,' *Lawfare*, (October 19, 2016). Retrieved from: https://www.lawfareblog.com/still-more-loud-cyber-weapons.

Lindsay, Jon R., 'Stuxnet and the Limits of Cyber Warfare,' *Security Studies*, 22:3 (2013), 365-404.

Mathew, S., R. Giomundo, S Upadyaya, M. Sudit, and A. Stotz, 'Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams' VizSEC '06, Proceedings of the 3rd International Workshop on Visualization for Computer Security (2016), 1-6.

Maurer, Tim, '"Proxies" and Cyberspace', *Journal of Conflict and Security Law*, 21:3 (2016), 383-403.

Maurer, Tim, 'Cyber Proxies and the Crisis in Ukraine,' in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (NATO CCD COE Publications: Tallinn, 2015).

McDonald, Geoff Liam O Murchu, Stephen Doherty, Eric Chien, 'Stuxnet 0.5: The Missing Link,' *Symantec*, (February 26, 2013). Retrieved from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.p.

Monahan, Torin, 'The murky world of 'Fusion Centres',' *Criminal Justice Matters*, 75:1 (2009), 20-21.

Morgus, Robert 'Whodunnit? Russia and Coercion Through Cyberspace,' *War on the Rocks*, (October 19, 2016). Retrieved from: http://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/.

Nakashima, Ellen 'Obama moves to split cyberwarfare command from the NSA,' *Washington Post*, (December 23, 2016). Retrieved from: https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html?utm_term=.8dba21add7e9.

National Cyber Security Centrum, 'Cybersecuritybeeld Nederland CSBN 2016,' (2016). Retrieved from: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html.

Pellerin, Cheryl, 'New Threat Center to Integrate Cyber Intelligence,' US Department of Defense, (February 11, 2015). Retrieved from: https://www.defense.gov/News/Article/Article/604093.

Polanyi, Michael, *Personal Knowledge: Towards a Post-Critical Philosophy*, (University of Chicago Press, Chicago: 1958).

Pomerleau, Mark 'Services integrating cyber and traditional military forces,' (September 30, 2016). Retrieved from: http://www.c4isrnet.com/articles/services-integrating-cyber-and-traditional-military-forces.

Rid, Thomas, *Cyber War Will Not Take Place*, (C. Hurst & Co: London: 2013), 83-84.

Rid, Thomas and Ben Buchanan, 'Attributing Cyber Attacks,' *Journal of Strategic Studies*, 38:1-2 (2015), 4-37.

Sanger, David, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Random House: New York: 2012).

Seagraves, J.A. and C.E. Bishop, 'Impacts of Vertical Integration on Output and Industry Structure,' *Journal of Farm Economics*, 40 (1968), 1814-1827.

Segal, Adam 'Takeaways from a Trip to the National Security Agency,' *Council on Foreign Relations*, (December 21, 2016). Retrieved from: http://blogs.cfr.org/cyber/2016/12/21/takeaways-from-a-trip-to-the-national-security-agency/.

Shea, Jamie, 'Lecture 6 - Cyber attacks: hype or an increasing headache for open societies?' (February 29, 2012). Retrieved from: http://www.nato.int/cps/en/natolive/opinions_84768.htm.

Smeets, Max, 'What it Takes to Develop a Cyber Weapon,' Columbia University. SIPA: Tech & Policy Initiative, Working Paper Series 1 (2016), 49-67.

Smeets, Max, 'A Matter of Time: On the Transitory Nature of Cyber Weapons,' *Journal of Strategic Studies*, (2017), 1-28.

Tang, Shiping, 'The Security Dilemma: A Conceptual Analysis,' *Security Studies*, 18:3 (2009), 587-623.

The Netherlands Ministry of Justice, 'De Nationale Cybersecurity Strategie 2: Van bewust naar bekwaam,' (2013, October).

The Netherlands Ministry of Defense, 'Cyber Command'. Retrieved from: https://www.defensie.nl/english/topics/cyber-security/contents/cyber-command.

Thompson, James D., *Organizations in Action: Social Science Bases of Administrative Theory*, (McGraw-Hill: 1967).

Tritak, John, 'Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems?' hearing before the committee on Energy and Commerce, (April 5, 2001).

Truman, Gregory E., 'Integration in electronic exchange environments,' *Journal of Management Information Systems*, 17:1 (2000), 209-244.

UK Government, National Cyber Security Strategy 2016-2021, (2016). Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

US Department of Defense, 'Joint Concept on Cyberspace - US Department of Defense,' (2011).

US Department of Defense, 'The DoD Cyber Strategy,' (April 2015).

Waltz, Kenneth, *A Theory of International Politics*, (New York: McGraw-Hill, 1979).

Woods, Ngaire, *The Globalizers: The IMF, the World Bank and their Borrowers,* (Ithaca, NY: Cornell University Press, 2006).

Yould, Rachel, 'Beyond the American Fortress: Understanding Homeland Security in the Information Age'. In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. (The New Press: 2003).

Zetter, Kim, 'Inside the Cunning Unprecedented Hack of Ukraine's Power Grid,' *Wired*, (2016). Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zetter, Kim, 'We are at Cyberwar: A global guide to nation-state digital attacks,' *Wired*, (2015). Retrieved from: https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/.