Toward an Ambidextrous Framework for Offensive Cyberspace Operations: A Theory, Policy and Practice Perspective

Gazmend Huskaj[1] and Ion A. Iftimie[2]
[1]Swedish Defence University, Stockholm, Sweden; School of Informatics, University of Skövde, Sweden
[2]Eisenhower Defence Fellow, NATO Defense College, Rome, Italy; European Union Research Center, George Washington School of Business, Washington, D.C.; Central European University, Vienna, Austria
gazmend.huskaj@fhs.se
iftimie@gwu.edu
DOI: 10.34190/ICCWS.20.052

Abstract: This article addresses the rise in state-sponsored cyber attacks over the past three decades and proposes a new ambidextrous framework for offensive cyberspace operations. Since 1982, nation states have embarked in a fierce race to develop both clandestine and covert offensive cyber capabilities. Their intended targets range from foreign militaries and terrorist organizations to civilian populations and the critical infrastructures that they rely upon. Advancements in cyber security have, however, contributed to the discovery and attribution of offensive cyber operations, such as state-sponsored ransomware attacks, where state-built cyber capabilities have been used to attack governments, industries, academia and citizens of adversary nations. The financial and psychological costs of these ransomware attacks are today a threat to any state's national security. This article draws from academic research, the cyber military doctrines of four countries—a total of eight models from the Netherlands, Sweden, the U.S., and the U.K.—and the authors' operational experience to propose a new ambidextrous framework for offensive cyberspace operations. This ambidextrous framework for offensive cyberspace operations and the associated Cyberspace Operations Canvas are needed today in order to increase the resilience of national critical infrastructures against attacks from state-developed tools. We use the WannaCry-case to illustrate how the implementation of the ambidextrous framework for offensive cyberspace operations would result in increased awareness and understanding of the prospective cyber threats, their intended target(s), the likelihood of cascading effects and the options available by nation states to minimize them.

Keywords: Ambidextrous Framework for Offensive Cyberspace Operations, Critical Infrastructure Protection, Cyberspace Operations Canvas, Cyber Resilience, State-Sponsored Cyber-Attacks, WannaCry

1. Introduction

In 1982, President Ronald Reagan directed William Casey, his Director of Central Intelligence, to discredit the integrity of the Soviet Trans-Siberian (Urengoy–Pomary–Uzhhorod) gas pipeline and dissuade Western European allies from supporting the project. A clandestine and covert operation was soon authorized to use a Trojan horse against the program operating "the pumps, turbines, and valves" of the pipeline. The state-built Trojan horse "reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds" (Reed 2005). In June of that same year, the cyber attack caused an explosion with "the power of a three-kiloton nuclear weapon" during a routine pressure test (Byres and Eng 2009, 58).

Since 1982, nation states have embarked in a fierce race to develop both clandestine and covert offensive cyber capabilities. Their intended targets range from foreign militaries and terrorist organizations to civilian populations and the critical infrastructures that they rely upon. Recent advancements in cyber security have, however, contributed to the discovery and attribution of offensive cyber operations, such as state-sponsored ransomware attacks, where state-built cyber capabilities have been used to attack governments, industries, academia and citizens of adversary nations. The financial and psychological costs of these ransomware attacks are today a threat to any state's national security. For example, the North Korea-attributed WannaCry-attacks used the EternalBlue software, an offensive cyber capability developed by a nation state to exploit flaws in the SMB-protocol. In the United Kingdom, the WannaCry malware affected many private companies, universities and even public critical infrastructures—such as the National Health Service hospitals—by encrypting their information systems and demanding a ransom to reopen them. Multiple cities in the United States have also been hit by the same type of attacks; yet, no national strategies have emerged to defend private and/or public critical infrastructures from state-sponsored cyber attacks. To date, there is very little academic research on models for offensive cyberspace operations (OCO).

This article draws from cyber military doctrine and the authors' operational experience to propose a new ambidextrous framework for OCO, which is needed today in order to increase the resilience of national critical infrastructures. Organizational ambidexterity is defined as the capacity of the organization "to simultaneously achieve alignment and adaptability" (Gibson and Birkinshaw 2004) at the organization level. Ambidextrous cybersecurity (AMBI-CYBER) "focuses on the protection of data, systems, and networks, while fostering the rapid introduction of new technologies" within an organization (Carayannis et al 2019). The purpose of the proposed ambidextrous framework for OCO is not to facilitate the destruction of adversary military infrastructure, but rather to enable a military organization in rendering an adversary (both military and non-military) incapable to conduct an attack (both in cyberspace and in the physical domain). In addition, we use case studies to illustrate how the implementation of the proposed ambidextrous framework to adversary attacks would result in increased organizational awareness and understanding of the prospective cyber threats, their intended target(s), the likelihood of cascading effects and the options available by nation states to minimize them. Our objectives are:

Objective 1: To investigate the current landscape of OCO models and frameworks; and
Objective 2: To develop a more comprehensive ambidextrous framework for OCO that better addresses growing state-sponsored cyber threats.

The research questions (RQ) this article addresses are:
RQ1. How much activity has there been to generate OCO models and frameworks?
RQ2. Who is leading the academic research in OCO models and frameworks?
RQ3. How should an ambidextrous OCO model and framework look like?

The methodology for this research is described in Section 2 and the results are presented in Section 3. Section 4 presents the answers to the research question, followed by conclusions in Section 5.

2. Methods

OCO academic research has not been common until recently (Huskaj 2019; Iftimie 2019). Instead, academic research has been focused on computer network operations (CNO), computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA). This article has been undertaken as a review of national cybersecurity strategies and of peer-reviewed articles in the field.

While OCOs have been conducted for over three decades, their legality during times of peace has not been publicly discussed by the General Counsel of the United States Department of Defense until January 19, 2017, through a memorandum to United States Combatant Commands titled "International Law Framework for Employing Cyber Capabilities in Military Operations" (Efrony and Shany 2018). This memo is significant, because it rejected the notion of sovereignty in cyberspace and concluded that "state cyber operations that interfere with the integrity of cyber infrastructure without the consent of a territorial State, that intrude into such cyber infrastructure, or perhaps even that alter such systems or their data without effects amounting to force or intervention do not amount to internationally wrongful acts" (Watts and Richard 2018, 830).

This legal interpretation is significant because it justifies the promotion of offensive cyber capabilities in national cybersecurity strategies. The United States Department of Defense (DOD) 2015 Cybersecurity Strategy, for example, calls for "building capabilities for effective cybersecurity and cyber operations", to include offensive cyber weapons (Miller et al. 2019). According to DoD, these tools are used so that cyber adversaries "lose confidence in their networks, to overload their networks so that they can't function, and do all of these things that will interrupt their ability to command and control forces" (Lin and Zegart 2019, 2017). Since then, almost a third of European Union member states mention the development of offensive cyber capabilities in their national cybersecurity strategies. None of them, however, indicate a preferred OCO model or process.

The peer reviewed literature has been selected using a computational literature review (CLR) based on the work by Mortenson & Vidgen (2016). The CLR "automates some of the analysis of research articles with analysis of impact (citations), structure (co-authorship networks) and content (topic modelling of abstracts)" (Mortenson & Vidgen, 2016, p. 1248). Impact analysis is derived by counting the total citations of individual articles (Mortenson & Vidgen, 2016). Further impact analysis is as follows:

> *For author impact the CLR provides: a total citation count; an impact factor calculated as the total citation count divided by the total number of papers; and, an h-index. For source impact, the CLR provides: a total citation count; and, an overall impact metric (total number of citations divided by number of papers)* (Mortenson & Vidgen, 2016, p. 1249).

The search process was a semi-automated search. The Scopus® database was queried using the search term ((offens* AND cyber* AND operation*) AND (model) OR (process)). The database results were 47 abstracts. Next, articles with no abstract and author were removed, resulting in 46 abstracts. Then, removing articles prior 2010 (that were no longer deemed current), resulted in 41 remaining abstracts. The manual part of the process involved validating the automated results. The 41 articles were imported into R and the CLR was applied. The `ldatuning`-algorithm showed that 25 topics existed. The topics and related abstracts that did not match the inclusion criteria were discarded. The remaining abstracts were then 13. Next, the 13 articles were acquired and manually evaluated. Seven articles remained. The conference venue names were harmonized, i.e. the year and proceedings were removed, and only the venue name was kept (see table 1).

Table 1: Selected journals and conference proceedings

ACM International Conference Proceeding Series	**International Conference on Cyber Warfare and Security, ICCWS**
Advances in Information Security	Journal of Defense Modeling and Simulation
CEUR Workshop Proceedings	Journal of Strategic Studies
Communications in Computer and Information Science	Lecture Notes in Computer Science
European Conference on Information Warfare and Security, ECCWS	Neurocomputing
Human Factors and Ergonomics Society	Philosophy and Technology
IEEE International Conference on Technologies for Homeland Security, HST 2012	Politics and Governance
IEEE International Scientific Conference on Informatics, INFORMATICS 2017 - Proceedings	Russian journal of criminology
IEEE Military Communications Conference MILCOM	SPIE - The International Society for Optical Engineering
International Conference on Availability, Reliability and Security, ARES 2011	Spring Simulation Interoperability Workshop
International Conference on Cyber Conflict, CYCON	Texas Law Review

This research then identified the peer-reviewed articles with a defined OCO model or process. Articles that did not fulfil the above criteria were excluded. Examples include articles that discussed offensive operations but were discussing simulation environments without a defined OCO model or process.

3. Results

This section presents the results of the impact analysis and the different OCO models identified. The results of impact analysis include the top articles ranked by citation counts (table 2), top publication venues (table 3) and top authors ranked by citation count and corpus-specific *h*-index. Table 2 presents the top articles by citation count. It notes that Grant et al. (2012) article titled "comparing models of offensive cyber operations" has most citation counts. What is noteworthy here is that research on models for offensive operations is led by Dutch researchers.

The publication venue for research on models for offensive operations is the International Conference on Cyber Warfare and Security (ICCWS). Table 3 presents the publication venues in the data set in order of *h*-index, number of articles, citations, the start and end year of publishing articles on models for offensive operations, the impact and the average papers per year. ICCWS leads on research about models on offensive operations with five articles and 13 citations, impact (an *h*-index of 2). ICCWS also has a higher impact (an impact of 2.6) and publishes 0.625 papers per year on the topic of OCO models. CYCON on the other hand has less articles published on OCO models. Authors have started to publish later on the OCO topic and do not publish consistently on OCO models.

Table 2: Top articles ranked by citation count (2 of 7 articles have zero citations)

Authors	Title	Year	Source	Cites
Grant T., Burke I., Heerden R.V.	Comparing models of offensive cyber operations	2012	International Conference on Cyber Warfare and Security, ICCWS	7
Grant T., Prins R.	Identifying tools and technologies for professional offensive cyber operations	2013	International Conference on Cyber Warfare and Security, ICCWS	4
Ducheine P., Van Haaster J.	Fighting power, targeting and cyber operations	2014	International Conference on Cyber Conflict, CYCON	3
Grant T.	Speeding up planning of cyber attacks using AI techniques: State of the art	2018	International Conference on Cyber Warfare and Security, ICCWS	1
Burke I., Van Heerden R.P.	Automating cyber offensive operations for cyber challenges	2016	International Conference on Cyber Warfare and Security, ICCWS	1
Grant T.	Building an ontology for planning attacks that minimize collateral damage: Literature survey	2019	International Conference on Cyber Warfare and Security, ICCWS	0
Moore D.	Targeting technology: Mapping military offensive network operations	2018	International Conference on Cyber Conflict, CYCON	0

Table 3: Analysis of publication venues

Source title	Articles	Cites	Start year	End year	Impact	Papers/year	*h*-index
International Conference on Cyber Warfare and Security, ICCWS	5	13	2012	2019	2.6	0.625	2
International Conference on Cyber Conflict, CYCON	2	3	2014	2018	1.5	0.4	1

The leading author conducting research on OCO models is Grant T. Table 4 also shows that the author Grant T. has been cited 12 times and has leading impact (an *h*-index of 2). This suggests that Grant T. is leading the research on OCO models.

Table 4: Analysis of Grant T. publications in ICCWS

Source title	Articles	Cites	Start year	End year	*h*-index
Grant T.	4	12	2012	2019	2

3.1 The OCO models

This section presents the models for offensive operations. Table 5 depicts the models based on scientific research and table 6 depicts doctrine models. The models list only the top tier of each step for easier comparison between them. Grant's (2018) model discussed in his "Speeding up planning of cyber attacks using AI techniques: State of the art" was discarded. This is because the model listed there refers to his 2012 "Comparing models for offensive cyber operations." Table 5 depicts the models from the identified scholarly literature, comparing each step. Grant's models from 2012 and 2013 have no major differences in tasks, and none in steps. In step 1, the difference is between selecting goals (2012) and determining goals (2013). In step 4, the difference is between attack (2012) and counter-attack (2013).

Ducheine et al. (2014) OCO model may be considered a model for intelligence collection in cyberspace using OCO. This is due to the use of terminology (reconnaissance, camouflage and exfiltrate) but also the focus on covert behavior to conceal identity (camouflage), and to finally 'exfiltrate' information from a target.

Burke et al. (2016) OCO model is focused on attack. The steps 'target identification' and 'reconnaissance' are self-explanatory. However, 'ramp-up', 'damage', and 'residue' all are considered as part of an attack phase. 'Ramp-up' is an action taken either by a sensor or user. For example, a sensor can detect a vulnerability scan and a user can open a spear-phishing mail. 'Damage' can refer to sensors detecting web-defacement or an unauthorized user access.

Grant's (2019) model is also focused on attack. The first step, 'foot-printing and reconnaissance' is the same action: collect information about a target such as IP-addresses, VPNs, and domains. 'Target access' is about generating access to a target, such as through social engineering and beyond (Grant, 2019). The remaining steps are self-explanatory.

Moore (2018) applies the US Department of Defense Common Cyber Threat Framework (CTF). The CTF "defines preparation as all collective efforts to identify targets, develop capabilities, assess victim vulnerability and define the scope of the operation" (US DNI 2013, 2, as cited by Moore, p. 92). 'Engagement' is defined as "threat actor activities taken prior to gaining access but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores" (DNI US 2013, 4, as cited by Moore, p. 96). Moore (2018) sees this step as taking action on enemy networks. The 'presence' step is about establishing and maintaining presence by moving laterally (Moore, 2018). Finally, the 'effect' step is when "ordnance is activated, disabling, disrupting or manipulating targets" (Moore, 2018, p. 100).

Of note is that only Grant's two models (2012, 2013) begin by selecting or determining goals. None of the other models do so. Furthermore, some of the models in the literature focus more on intelligence collection than an obvious offensive action, but are still listed as OCO models. We have included these models here because before the actual process of intelligence collection in cyberspace occurs, an offensive cyber action must still be taken to gain access to the target.

Table 5: The models and their different steps

Author	Year	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
GrantT.	2012	Select goals	Select target(s)	Plan	Attack	Lessons learned	
GrantT., PrinsR.	2013	Determine goals	Select target(s)	Plan	Counter-attack	Lessons learned	
Ducheine P., Van Haaster J.	2014	Reconnaissance	Design	Intrusion	Action	Camouflage	Exfiltrate
Burke I., Van Heerden R.P.	2016	Target identification	Reconnaissance	Ramp-up	Damage	Residue	Post-attack
GrantT.	2019	Foot-printing & Reconnaissance	Planning	Target access	Penetration	Payload delivery	After action review
MooreD.	2018	Preparation	Engagement	Presence	Effect		

The reviewed doctrine models are from 1) the U.S.: Joint Publication (JP) 3-12, Army Doctrine Publication (ADP) 5-0, Air Force Doctrine Document (AFDD) 3-12, JP 5-0, 2) NATO: NATO Allied Joint Doctrine (AJP) 5, United Kingdom version, and NATO Operations Planning Process (OPP), Netherlands version, and 3) Sweden: Operativ Doktrin and the Svensk planerings- och ledningsmetod (SPL). The models depicted in table 6 vary. To showcase these differences, only Step 1 is presented. The remaining steps are left to the reader for consideration.

The first step involves 'planning' (model no. 1,2,8), 'situational awareness' or 'design' (models 3-6), 'indications & warning' (model no. 7), 'knowledge building' (model no. 10-12), and 'tasking' (model no. 13). This shows the discrepancies that exist among countries and among field manuals of the same nation. Merriam-Webster defines 'planning' as "the establishment of goals, policies, and procedures for a social or economic unit" (2019). 'Situation awareness' or 'design' means "the up-to-the-minute cognizance or awareness required to move about, operate equipment, or maintain a system" (Council, 1998, p.172). 'Indication' is defined as "a specific act or decision an enemy has taken as part of an aggressive action" (Goldman, 2001, p. 21) and 'warning' is defined as "a notification of impending activities that may, or may be perceived to, adversely affect U.S. national security interests or military forces" (Goldman, 2001, p. 38). 'Knowledge building' refers to "the process of creating new cognitive artifacts as a result of common goals, group discussions, and synthesis of ideas. These pursuits should advance the current understanding of individuals within a group, at a level beyond their initial level of knowledge, and should be directed towards advancing the understanding of what is known about that topic or idea" (Scardamalia & Bereiter, 2003, p. 5). While planning involves establishing

goals, policies and procedures, situation awareness is about up-to-the-minute information about the environment, and indication and warning (I&W) is about a notification of enemy aggressive actions. These three have different perspectives; planning involves own activities, situation awareness is about collecting information on the environment, and I&W is about an adversary's actions.

Table 6: Doctrine models and their different steps

No.	Author	Year	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
1	JP 3-12	2018	Plan	Coordinate	Execute	Assessment		
2	ADP 5-0	2012	Plan	Prepare	Execute	Continuously Assess		
3	AFDD 3-12	2011	Design	Plan	Execute	Assessment		
4	COPD	2013	Initial Situational Awareness of A Potential/Actual Crisis	Operational Appreciation of the Strategic Environment	Operational Estimate	Operational Plan Development	Execution	Transition
5	JP 5-0	2017	Situational Awareness	Plan	Execute	Assessment Activities		
6	NATO AJP-5 UK	2019	Situation Awareness	Operational appreciation	Operational Estimate	Operational appreciation	Execution	Transition
7	NATO OPP NL			Political-Military Estimate Process				
		2013	Indications & warning	Assessment	Response Options	Planning & Execution	Return to stability	
				Operational Planning Process				
8	Operativ Doktrin	2014	Plan	Execute	End of Operation	Assessment and LL		
9	SPL STRA-level	2017	Knowledge building	Mission Analysis	Military Strategic Assessment	Military Strategic Planning	Execution	End of Operation
10	SPL OP-level	2017	Knowledge building	Mission Analysis	Operational Assessment	Operational Planning	Execution	End of Operation
11	SPL Offensive-method	2017	Knowledge building	Assessment for Direction	Planning	Direct Control	Follow-up	Operational Evaluation
12	SPL Direct-method	2017	Knowledge building	Assessment for Direction	Planning	Follow-up	Operational Evaluation	
13	SPL Figure 51	2017	Task	Analysis	Assessment	Planning	Execution	End of Operation

The authors' model has gone through five iterations. The first version was developed by considering research and doctrine models, coupled with the authors' own experience conducting military and intelligence operations in deployed theatres. Table 7 depicts the various versions. Version 1 begins by understanding the adversary. This entails collection on threat actors, intent, and capabilities. Planning timelines is about the required intelligence on threat actors' targets, any identified vulnerabilities, which are required to start the secure engineering development process (SEDPro), and for policy support. Characteristics of cyberspace capabilities are the requirements on the SEDPro. The requirements are derived from the intelligence collected on the adversary target(s) information systems. Examples of requirements include operating system type and version, web server type and version, the purpose of the information system, and its value to the adversary.

Cascading effects are the potential risks that the developed software goes beyond its target system and spreads, but also that its use is proportionate according to the law of armed conflict (JCS, JP3-12, 2018). Reversibility of effects is "the level of control over the duration of the effect that can be exercised by friendly forces" (JCS, JP3-12 2018, p. IV-3). Version 2 of the model was derived as a result of an interview with an expert in cyberspace operations. The respondent stated that before understanding the adversary, you need something that triggers the process, like a problem or threat. This resulted in adding that to Version 2 of the model as Step 1. Version 3 of the model was revised by switching places between Step 1 and 2, but also by

moving Cascading Effects and Reversibility of Effects from their respective steps (5 and 6), to Step 4. Furthermore, Execute and End / Lessons Learned were added to Version 3.

In Version 4 of the model, a new interview was conducted where the results of the interview led to removing the "What is the problem/threat?" step. The underlying reason was that "there are too many problems, it's more realistic to prioritize on adversary intent and capability." In version 5 of the model, to highlight the importance of policy support and intelligence support, these two were added as continuously supporting the model. The model went another major revision resulting in Version 6. A half-day workshop was held discussing the model and the various steps in it. The model was cut down from five steps to four. In addition, each of the steps, excluding Step 2, received new titles (Indicators & Warning, Operational Considerations, and Decision Point). Furthermore, EXECUTE and NO / GO were added under Step 4.

A note on why Indicators & Warning is the first step, and not Targeting or any other action which may be considered as "throwing the first punch." The paradigm in which western countries reside in is a rule-based international order. Russia for example, is considered as a middling power disregarding international institutions (Brown, 2019), while China is attempting to subvert rule-based international order in regards to human rights (Parliament, 2019). Finally, a note on the SEDPro. The purpose is to develop the software which is used to deny, degrade, disrupt, destroy or manipulate in a secure way. The development is based on certain pre-defined requirements derived from collection on a target. Next, it needs to be evaluated to assure that it conforms to the requirements.

Table 7: The authors' model and revisions, from one (1) to six (6)

Version	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
1	Understand the Adversary	Planning Timelines	Characteristics of Cyberspace Capabilities	Cascading Effects	Reversibility of Effects	
2	What is the problem/threat?	Understand the Adversary	Planning Timelines	Characteristics of Cyberspace Capabilities	Cascading Effects	Reversibility of Effects
3	Understand the Adversary	What is the problem/threat?	Planning Timelines	Characteristics of Cyberspace Capabilities Cascading Effects Reversibility of Effects	Execute	End / Lessons Learned
4	Understand the Adversary	Planning Timelines	Characteristics of Cyberspace Capabilities Cascading Effects Reversibility of Effects	Execute	End / Lessons Learned	
5	**Policy Support**					
	Understand the Adversary	Planning Timelines	Characteristics of Cyberspace Capabilities Cascading Effects Reversibility of Effects	Execute	End / Lessons Learned	
	Intelligence Support					
6	**Policy Support**					
	Indicators & Warning	**Planning Timelines**	**Operational Considerations**	**Decision Point**		
	Commander's Intent	Key Resources	Key Operational Activities	Risks for Cascading Effects?		
	End State	Operation Value Proposition	Operational Channels	Deconfliction		

Version	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
	Motives	Target Profiles	Operational Investments	EXECUTE / NO GO		
	Operation Key Partners	Deconfliction	Risk & Challenges			
	Intelligence Support			B(yte)DA		

4. Discussion

This section discusses the objectives and the answers to the research questions. The results have demonstrated that many different models for military operations exist and they differ. It also turns out that some models which are dubbed as OCO models have emerged from intelligence collection operations in cyberspace. Investigating the first objective "to investigate the current landscape of OCO models and frameworks" reveals that the leading scholars conducting academic research on OCO models are from the Netherlands and South Africa. The second objective to "To develop a more comprehensive OCO framework that better addresses growing state-sponsored cyber threats" is depicted in Table 7, Version 6.

RQ1. *How much activity has there been to generate OCO models and frameworks?*
Six models for offensive operations have been generated from the articles in table 2. These models have been driven by scholars in the field of cyberspace operations. Table 5 depicts the steps in these models. It has already been mentioned that one model was developed specifically for intelligence collection. Next, there are also the models generated by military Doctrine. Four countries and one organization were chosen for this study. In alphabetic order, the Netherlands, Sweden, the U.S., and the U.K. have produced eight models. However, these models have been developed for military strategic and operational level operations. They have not been explicitly produced for cyberspace operations, except for Joint Publication 3-12 (U.S.).

RQ2. *Who is leading the academic research in OCO models and frameworks?*
The leading scholars conducting academic research on models for offensive cyberspace operations are from the Netherlands and South Africa (a direct result of government and academia collaboration in the writing of military field manuals within these countries). The scholars' preferred venue to publish scientific research on models for offensive operations is ICCWS, followed by CYCON. However, even though the initial search shows that other venues for publication exist (table 1), those venues do not have the same focus as ICCWS and CYCON.

RQ3. *How should an ambidextrous OCO model and framework look like?*
Version 6 in Table 7 shows the current OCO models/frameworks. It has been produced by surveying models for operations in military doctrine and the authors' operational experience. Next, the model has been evaluated and revised multiple times by discussing it with experts in cyberspace operations, and then revised during a half-day workshop. The model will now be applied to the WannaCry-case with the accompanied tool: the Cyberspace Operations Canvas. It should be noted that some assumptions have been made regarding the WannaCry-case. These include, End State, Motives, Operation Key Partners, Deconfliction, Key Operational Activities, Operational Investments, Risk & Challenges, and Battle Damage Assessments—or Byte Damage Assessments, B(yte)DA.

Cyberspace operations canvas

Operation name: WannaCry		**PURPOSE:** Financial gain for the North Korean government.	
Indicators & Warning		**Planning Timelines**	
Commander's Intent (Lazarus Group)	Financial Gain	Key Resources	Personnel, Cyber Capability (EternalBlue, DoublePulsar)
End State	Show of force	Operation Value Proposition (what effects can the operation generate?)	Deny, Destroy
Motives	Perceived threats to North Korea	Target Profiles	Various organisations using Microsoft Windows with SMBv1.0
Operation Key Partners	None	Deconfliction	None

Operation name: WannaCry		**PURPOSE:** Financial gain for the North Korean government.	
Operational Considerations		**Decision Point**	
Key Operational Activities		Risks for Cascading Effects?	Yes. The software has worm-capabilities and exploits SMBv1.0
- intel collection	Use existing collection channels.	Deconfliction	None required. Policy supports us
- target selection	Targets selected if they have SMBv1.0-vulnerability.	EXECUTE / NO GO	EXECUTE
- characteristics of cyber capabilities	EternalBlue: ransomware, worm DoublePulsar: backdoor	B(yte)DA	Follow operation through Media-reporting
- cascading effects	Yes		
- reversibility of effects		No	
Operational Channels			
- who supports the operation?		None	
- how will we reach the targets?		attack infrastructure, Encrypted Tor C2-servers	
- how will we deliver the payload?		exploit SMBv1.0 vulnerability, worm capabilities	
Operational Investments			
- how much will it cost to develop:		No cost, get it from Shadow Brokers	
- maintain op:		No cost, fire and forget.	
- operate op:		No cost, fire and forget.	
Risk & Challenges			
- Political risk:		None, deny any allegations	
- Uncertain effects:		None. Every machine that is encrypted is a potential income	
- High technology requirements:		None	
- Legal officer:		None. North Korea supports operations for financial gain	

The above Cyberspace Operations Canvas answers the research question *How should an ambidextrous OCO model and framework look like?* A strength of the Cyberspace Operations (CO) Canvas is that it was built based on the work of Osterwalder (2010) and Rose et al. (2019) with Boyd's OODA-loop in mind; and adapted for offensive cyberspace operations.

5. Conclusions

This research addressed the rise in state-sponsored cyber attacks over the past three decades with the aim to contribute to the body of knowledge on offensive cyberspace operations. With only 13 peer-reviewed articles addressing offensive cyberspace operations frameworks, there is additional room for research on the field. Starting with these articles, a new ambidextrous framework for offensive cyberspace operations was proposed, which also draws from the cyber military doctrine in four countries (United States, United Kingdom, Netherlands, and Sweden) and the authors' operational experience. We argue that the new ambidextrous framework for offensive cyberspace operations is needed today in order to increase the resilience of national critical infrastructures. We used WannaCry as a case study to illustrate how the implementation of the proposed ambidextrous framework for offensive cyberspace operations would result in increased awareness and understanding of the prospective cyber threats, their intended target(s), the likelihood of cascading effects and the options available by nation states to minimize them. One limitation of this research is that it is based on limited information available to the public about how nations conduct offensive cyberspace operations. Therefore, an analysis of more articles on models for Computer Network Attack (CNA) may be useful in refining this ambidextrous framework in the future.

Acknowledgements

Gazmend wishes to thank Marcus Nohlberg, PhD, for his ideas on the workshop and canvas.

References

Brown, James. (2019). Why Russia should learn to love the rules-based international order. Retrieved from https://www.opendemocracy.net/en/odr/why-russia-should-learn-love-rules-based-international-order/.

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.

Byres, E. J., & Eng, P. (2009). "Cyber Security and the Pipeline Control System." Pipeline & Gas Journal, February. https://www.tofinosecurity.com/sites/default/files/Cyber_Security_and_The_Pipeline_PGJ_Feb_2009.pdf.

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2019). Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. IEEE Transactions on Engineering Management.

Council, N. R. (1998). Modeling Human and Organizational Behavior: Application to Military Simulations (R. W. Pew & A. S. Mavor, eds.). https://doi.org/10.17226/6173. Retrieved from https://www.nap.edu/read/6173/chapter/9.

Department of the Army. (2012). ADP 5-0 The Operations Process.

Ducheine, P., & Van Haaster, J. (2014). Fighting power, targeting and cyber operations. International Conference on Cyber Conflict, CYCON, 2014, 303–327. https://doi.org/10.1109/CYCON.2014.6916410

Efrony, D., & Shany, Y. (2018). "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice." The American Journal of International Law 112 (4): 583–657.

Försvarsmakten. (2014). Operativ Doktrin 2014.

Försvarsmakten. (2017). Svensk planerings- och ledningsmetod 2017.

Gibson, C. B., & Birkinshaw, J. (2004). "The antecedents, consequences, and mediating role of organizational ambidexterity." Academy of management Journal 47, No. 2: 209-226.

Goldman, J. (2001). Joint military intelligence: Intelligence Warning Terminology. Retrieved from https://www.hsdl.org/?view&did=7443

Grant, T. (2018). Speeding up planning of cyber attacks using AI techniques: State of the art. Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018, 2018-March(March), 235–244.

Grant, T. (2019). Building an Ontology for Planning Attacks that Minimize Collateral Damage: Literature survey. (March), 78–86.

Grant, T. J. (2013). Identifying 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.

Huskaj, G. (2019). "The Current State of Research in Offensive Cyberspace Operations." Proceedings of the 18th European Conference on Cyber Warfare and Security. Edited by Tiago Cruz and Paulo Simoes. ACPI: Reading, UK, pp. 660–667.

Iftimie, Ion A. 2019. "Cyber Sanctions: The Embargo of Flagged Data in a Geo-Cultural Internet." Proceedings of the 18th European Conference on Cyber Warfare and Security. Edited by Tiago Cruz and Paulo Simoes. ACPI: Reading, UK, pp.668-676.

Joint Chiefs of Staff. (2018). Joint Publication 3-12 Cyberspace Operations. Retrieved from https://fas.org/irp/doddir/dod/jp3_12.pdf

Joint Force Development JFD, & JFD, J. F. D. (2017). Joint Publication 5-0. (June 2017), 360. Retrieved from https://fas.org/irp/doddir/dod/jp3_57.pdf

Lin, H., & Zegart, A. (2017). "Introduction to the Special Issue on Strategic Dimensions of Offensive Cyber Operations." Journal of Cybersecurity 3 (1): 1–5.

Lin, H., & Zegart, A. (2019). Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. Brookings Institution Press.

Merriam-Webster (2019). Planning. Retrieved from https://www.merriam-webster.com/dictionary/planning.

Miller, K., O'Halloran, B., Pollman, A., & Feeley, M. (2019). "Securing the Internet of Battlefield Things While Maintaining Value to the Warfighter." In International Conference on Cyber Warfare and Security, 546–53. Academic Conferences International Limited.

Ministerie van Defensie. (2013). Joint Doctrine Publication 5: Command and Control. Retrieved from https://www.defensie.nl/documenten/publicaties/2012/03/16/joint-doctrine-publication-5-command-and-control-en

Moore, D. (2018). Targeting technology: Mapping military offensive network operations. International Conference on Cyber Conflict, CYCON, 2018-May, 89–107. https://doi.org/10.23919/CYCON.2018.8405012

Mortenson, M. J., & Vidgen, R. (2016). A computational literature review of the technology acceptance model. International Journal of Information Management, 36(6), 1248–1259. https://doi.org/10.1016/j.ijinfomgt.2016.07.007

NATO. (2011). Allied Joint Doctrine for the Concept of Operations. Allied Joint Publication, 3(B)(UK joint doctrine).

NATO. (2013). Allied Command Operations Comprehensive Operations Planning Directive. Retrieved from https://www.forsvarsmakten.se/siteassets/english/swedint/engelska/swedint/courses/nato-copc/07-ch-4-op-v2.0-04-oct-13.pdf

Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation. Hoboken, New Jersey: Wiley & Sons.

Parliament. (2019). China and the Rules-Based International System. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/61203.htm.

Reed, T. C. (2005). At the Abyss: An Insider's History of the Cold War. Presidio Press.

Rose, J., Holgersson, J., Söderström, E. (2019). Designing Innovative Digital Services for Government: A Business Model Canvas Adaptation. 27th European Conference on Information Systems (ECIS2019), Stockholm-Uppsala, Sweden, 2019.
Scardamalia, M. & Bereiter, C. (2003). Knowledge Building. In Encyclopedia of Education (2nd ed. pp. 1370-1373). New York: MacMillan Reference.
USAF. (2011). Cyberspace Operations. U.S. Air Force Doctrine Document (AFDD) 3-12.
Watts, S., & Richard, T. (2018). "Baseline Territorial Sovereignty and Cyberspace." Lewis & Clark L. Rev. 22 (3): 771.