2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Recommendations for Enhancing the Results of Cyber Effects

Erwin Orye
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia
erwin.orye@ccdcoe.org

Olaf M. Maennel
Department of Computer Science
Tallinn University of Technology
Tallinn, Estonia
olaf.maennel@ttu.ee

Abstract: Cyber effects[1] should be considered an important tool in the toolbox of warfare for the commander of a military operation. This paper discusses the key elements required to enhance decision-making in cyber operations. Many different parameters influence the outcome, but only some of them are internally controllable. This paper outlines how to predict the outcome of cyber effects and how to measure that outcome. It gives advice on developing cyber effect capabilities and reflects on how to integrate cyber effects in a mission as lateral support. The authors recommend a set of best practices for enhancing cyber effects in modern warfare.

Keywords: *cyber, effect, prediction, measuring, achieving*

1. INTRODUCTION

Although the defender and the attacker each control only a very small part of the cyberspace they use, whoever can influence the portion of cyberspace used by the adversary has the potential to control the adversary [1].

Better estimation of the effects achieved by cyber operations will allow for an enhanced decision-making process and ultimately, increased control over the adversary [2]. This higher-quality estimation will also improve the ability to predict side-effects,

[1] An "effect" is a direct or indirect objective (intended) outcome of an action. In warfare, the actions are intended to create effects, typically against the functional capabilities of a material target or to the behaviour of individuals.

both those that might be useful and those that are unwanted and could cause collateral damage. In this paper we discuss the strategic aspects to be taken into account in order to develop cyber effect capabilities and discuss the importance of predicting and measuring the outcomes of cyber effects.

How to integrate cyber effects in a mission is not yet well defined. In traditional warfare domains, such as land, sea and air, there are well-defined procedures and streamlined information-sharing mechanisms for lateral support from one nation to another.

First, we provide an overview of how cyber effects can be measured and predicted. Next, we discuss how cyber effects can be achieved and enhanced. Finally, the authors provide a series of recommendations stressing the important role of collaboration in enhancing cyber effects in modern warfare.

2. STEP 1: MEASURING AND PREDICTING CYBER EFFECTS

To enhance the effectiveness of cyber operations, a continuous evaluation of the impact is needed to recommend changes to tactics, strategies, objectives, and guidance. The end state of a campaign is an original estimate that will be constantly modified during an operation. Cyber effects should be estimated in order to identify and quantify the impact of cyber operations in warfare, which is essential to predict an end state. In order to make adjustments during the cyber operation, the outcomes, also referred to as battlefield damage estimation in kinetic[2] warfare, need to be measured.

A. Scope

There is no commonly accepted definition of cyber war and cyber warfare, which indicates the difficulty of reaching such a definition. The terms computer information warfare (IW), (offensive) information operation (IO), and network attack (CNA) are frequently used interchangeably [3].

Cyber war basically refers to a sustained computer-based cyberattack by a state, state-owned organisation (e.g. NSA[3] or national CERT[4]) or state-sponsored organisation against the IT infrastructure of a target state.

[2] "Kinetic warfare" is used in this paper as an umbrella term to cover warfare that uses weapons that have mechanic, kinetic, thermal, radiological, biological, or chemical effects.

[3] National Security Agency

[4] Computer Emergency Response Team

Cyber warfare could be defined in different ways:

- As defending and attacking information and computer networks, as well as denying an adversary's ability to do the same, or even dominating the information environment on the battlefield. It can include computer or network penetration, denial-of-service attacks on computers and networks, equipment sabotage through cyberspace, sensor jamming, and even manipulating trusted information sources to condition or control an adversary's thinking [4].
- As the use of computers or network-based capabilities by a state, or a group or person whose actions can be attributed to a state, in order to launch an attack on another state [3].
- By means of essential characteristics it has to fulfil: "a cyber attack reaching the level of an armed attack or cyber activity occurring in the context of armed conflict." The essential characteristics of an armed attack are: "the objective must be to undermine the function of a digital information system or network" and that it "must have a political or national security purpose" [5].

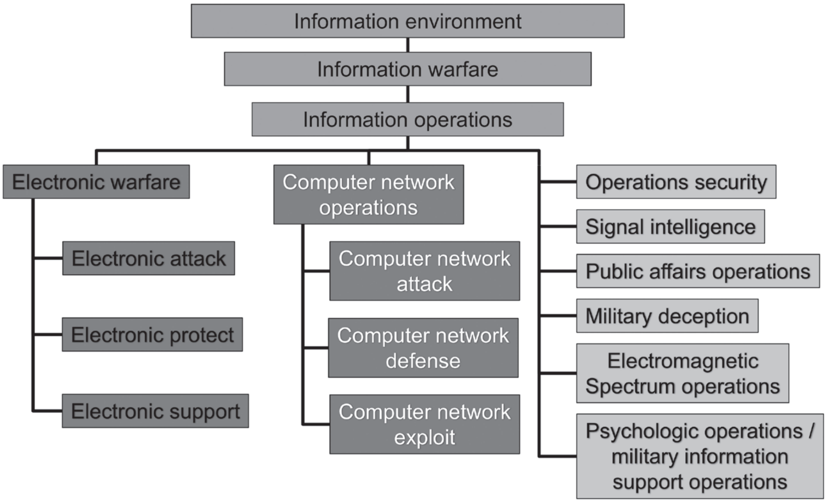
There is also no common agreed definition of information warfare. Figure 1 gives a non-exhaustive overview of information warfare and information operations. Definitions of information warfare could be:

- The use of information technology as an active weapon of war. This includes attempts to intercept, disrupt, and defend military-specific communications, information technology, and critical computer systems.
- The tactical and strategic use of information to gain an advantage.

There is still discussion over whether this is only conducting or defending against electronic attacks on computers and related information systems or whether it also includes the whole spectrum of possibilities for using information effectively in warfare and denying enemies the same capability [6].

Information operations are actions taken to affect adversary information and information systems while defending one's own. They are the integrated employment of the core capabilities of influence operations, electronic warfare operations, network warfare operations, together with specified integrated control enablers, to influence, disrupt, or corrupt adversarial human and automated decision-making while protecting our own.

FIGURE 1: INFORMATION OPERATIONS AND INFORMATION WARFARE [6]



Traditional warfare is characterised as a violent struggle for domination between nation-states or coalitions and alliances of nation-states, or, as Carl von Clausewitz put it in his book *On War* [7], war is "a mere continuation of policy by other means". This confrontation typically involves force-on-force military operations in which adversaries employ a variety of conventional military capabilities against each other in the air, land, maritime, and cyberspace domains. The objective may be to convince or coerce key military or political decision-makers, defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies [8].

The term "hybrid operations" describes a specific subset of strategy that employs conventional military force supported by irregular and cyber warfare tactics. For hybrid threats, the methods and activities are multidimensional and the links between different actions are unclear. Sometimes they are even impossible to verify. Hybrid threats as such fall short of hybrid warfare, but if they are not detected or responded to, hybrid warfare can ensue [9],Hybrid warfare can be defined as blending conventional warfare and irregular warfare, potentially including cyber warfare and information warfare.

B. Cognitive and physical effects and orders of effects

Like traditional kinetic operations, a cyber operation is likely to cause cognitive effects.[5] Many of the cyber operations we see today have cognitive effects without important physical effects [10]. Cognitive effects of cyber operations include:

[5] Often one equates the terms kinetic and lethal and the terms non-kinetic and non-lethal. There might be a correlation between them, but the other combinations do also occur. This notion is important for effects-based operations in cyber warfare.

sowing confusion, changing behaviour, modifying trust, changing (public) opinion, manipulation, etc. One recent example of this is the Cambridge Analytica data analysis case [11], where social media was used to influence people's behaviour. However, not every cyber operation causes cognitive effects. For example, if a cyber attack, the aim of which is only to exfiltrate information, is not noticed by the target, it does not have cognitive effects until its discovery. Many cyber-targeted attacks are not discovered quickly by the target [12].

Effects have causes and can, in turn, cause further effects. A large number of cause-effect "chains" can be created, based on a single causal event. Cascading effects within the same IT systems are still considered to be first-order effects. Second-order effects are effects outside the IT environment, but within an independent mission (e.g. a factory or an organisation). Those effects represent the indirect effect caused by system failures triggered by the cyber operation: businesses or operations are interrupted, or at least degraded. These second-order effects are not desirable during covert or stealth cyber operations. Third-order effects are long-term. They represent the overall result of the first-order and second-order effects, which may be a change of behaviour in humans or institutions, an impact on international relations or a financial impact. These are the cyber effects that have a profound impact on ongoing operations, on the mission itself, and eventually even on strategic or political levels. In estimating the outcome of a cyber operation, one should not only consider first-order effects, but also examine the relationships between systems in order to estimate second- and third-order effects, which are potentially even more important for the mission and which could have an impact on different levels [13], as explained in subsection 3B.

An example of the different orders could be the NotPetya attack that took place in 2017, where the first-order effects were getting a malware through tax software that companies and individuals required for filing taxes in Ukraine. Among others, there were second-order effects on companies such as Maersk, which had interruptions in its operations that caused financial impact. The third-order effects were that different nations issued statements attributing NotPetya to Russian state-sponsored actors and the United States sanctioned Russian organisations that were believed to have assisted the Russian state-sponsored actors with the operation [14].

C. Measuring the effects of cyber operations

Cyber operations are able to create physical and cognitive effects, and can manifest in various ways: as first-order or higher-order effects; directly or indirectly; immediately or delayed. However, feedback (target damage assessment) as to the success or failure of a cyber effect reaching its destination, or whether the payload had been executed, is not always clear. Relevant questions for measuring the effects of cyber operations:

- Is it possible to detect disturbances in systems, even if the operation itself cannot be immediately detected and characterised?
- What are the effects – intended and actual – of the cyber operation on our own mission's effectiveness, as well as on our strategic interests?
- Is measuring first-order effects, for example by exfiltration of data, possible? Exfiltration of data can be by means of a command and control channel, a beacon installed on the target that provides information about the status of the cyber operation, an insider that leaks data or information, or other means.
- If there is no other way of directly measuring the outcome of a cyber operation, are there measurable second- or third-order effects?

Where possible, traditional kinetic battle damage assessment should also be used for cyber operations in order to integrate cyber effects as much as possible in the traditional warfare terminology [15].

D. Estimating the effects of cyber operations

Many different parameters influence the outcome of a cyber operation, but only some of them are controllable. Examples of such parameters are: the training of friendly forces and adversary personnel in cyber operations, the ability of the adversary to defend its IT infrastructure, the complexity of the systems involved, the accessibility of the targeted system, and so forth. The use of more parameters in identifying and quantifying the effects of cyber operations will result in better predictions.

No process currently exists that is capable of estimating the overall outcome of a cyber operation at mission level. Research has begun, but is still in the early stages of development. There is currently no way to describe dependencies between mission objectives, mission activities, and measurable outcomes. Integrating cyber operations into the overall mission is, for the moment, less effective than desired [2]. The existing, publicly-available modelling schemes deal with very specific scenarios based on attack graphs [16], game theory [17]–[19], extensions to traditional models of combat [20], modelling and prediction of several system properties using Monte Carlo models [21], or practical guides on how to better defend IT systems [22]. It is probably hard to create a model in the first place, but even if the model creation were doable, it would still be hard to measure and to validate it.

Analysis techniques are crucial in determining the decision metrics required to estimate the potential effects of cyber operations. In the development of decision metrics, the following is essential: physical or digital paths toward the final target, estimation of the probability of success, judgment about the amount of collateral damage that might be caused, and assessment of likely first-, second-, and third-order effects.

A framework for assessing cyber war that builds on the elements of risk assessment was proposed by Dorothy Denning [23]. However, for such a framework to be useful, as stated in the paper, there is a need for measurable metrics. In order to develop those decision metrics, one could use information security modelling and simulation tools to simulate a system's security baseline configuration and then test the outcome of the cyber effect in a simulated environment. There is a lack of publicly-available documentation about modelling methods and metrics for missions in cyberspace. Some likely reasons are:

- Test data is needed to validate a model or a technique, however data is not abundantly available for a mission and could be of a confidential nature.
- Impacts are often difficult to measure, even in laboratory conditions. Defining which parameters are relevant to measure is in itself a complicated matter, certainly for cognitive impacts, collateral damage and higher order effects.
- Cyberspace is highly dynamic, and often asymmetrical in nature [24].
- Rapid evolution of software and patching policies makes it harder to keep the cyber effects of technical solutions up to date and could reduce the time available for simulation.
- Most nations are developing internal capabilities due to the very sensitive nature of the topic. Therefore, there is no amplification factor of knowledge through information sharing.

E. Estimating the collateral damage of cyber operations

Like conventional kinetic weapons, cyber effects can cause collateral damage. In kinetic warfare, collateral damage is well understood, and policy, procedures, and national and international legislation are available. Collateral damage occurs when a military action causes unintended physical damage to civilian persons or objects [25]. Collateral damage in this context is not only used in relation to war and the laws of armed conflict, but also below this threshold with the prohibition of the use of force among states. When estimating the outcome of a cyber operation, collateral damage is a factor that must be taken into account. More and more, existing international law is accepted as applicable in cyberspace (at least by western societies) [26].

An example of regulation from the US Department of Defense clearly stipulates the procedure to avoid unnecessary collateral damage [27]:

- Identify the target.
- Determine whether protected persons or objects are within range of the target.
- Estimate the collateral damage that will occur.

- Determine whether there are other weapons that can accomplish the objective with less collateral damage.
- Evaluate whether the anticipated collateral damage exceeds the concrete and direct military advantage. Advantages that are hardly perceptible or would only appear in long-term view are to be disregarded.

This rule set is also applicable to cyber warfare or a cyberattack, but estimating the collateral damage that occurs might be very difficult to achieve in certain cases. Questions to take into consideration before planning cyber operations are:

- What to do when an operation unintentionally modifies data? What is the relevance and importance of the data concerned? Is the data related to lifesaving or loss of life? Can altering the data cause physical injury? Does the data contain private information? Has the data a military use?
- Is it possible to predict the outcome with confidence?
- What if the cyber effect, even after a long period of time, penetrates friendly forces in national industry or governmental institutions? In other words, is it possible that our own systems are vulnerable?
- Can the second- and third-order effects be predicted?

Although in theory IT systems should be deterministic as they are built on logic, in practice it is currently not possible to formally analyse a complete IT system, due to their complexity. They are often a system of systems and the components, hardware and software, are mostly built by different manufacturers. Even installation on site is often done by a wide range of employees from different companies. The effect of a cyber operation on such a complex system and the subsequent cascading effects are hard to predict.

Up to now, legal entities have not engaged much with this issue [28]. The *Tallinn Manual 2.0* states [29]in “Rule 113 – Proportionality” that “The issue is of particular relevance in the context of cyber attacks in that it is sometimes quite difficult to reliably determine likely collateral damage in advance”. It has to be mentioned that stress, irritation, fear or inconvenience are not considered as collateral damage, but cyber operations can cause those effects. There are examples where measures were taken to limit the collateral damage: for example, by assuring that the cyber operation is specific enough to affect only the target and will become inactive after a specific date, collateral damage can be reduced [30]. The following questionnaire, based on one created by the Obama administration in 2014 [31], is useful for estimating the impact of cyber collateral damage:

- How much is the targeted vulnerability present in the core IT infrastructure, in critical IT infrastructure, in coalition members' IT infrastructure, and in national IT systems?
- Does the vulnerability, if left unpatched, pose significant risk for national or allied systems (military and civilian)?
- Does the cyber effect impact the complete system or only specific subsystems?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- Does patching this vulnerability provide information that can be used by adversaries?
- How likely is it that we would know if someone else was exploiting this vulnerability?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Could we utilise the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

3. STEP 2: ACHIEVING CYBER EFFECTS: ENDS, WAYS, AND MEANS

According to Major General Dennis Laich [32]:

> "Ends are defined as the strategic outcomes or end states desired. Ways are defined as the methods, tactics, and procedures, practices, and strategies to achieve the ends. Means are defined as the resources required to achieve the ends, such as troops, weapons systems, money, political will, and time. The model is really an equation that balances what you want with what you are wiling [sic] and able to pay for it or what you can get for what you are willing and able to pay."

This section will comment on how the traditional application of 'ends', 'ways' and 'means' deviates from traditional warfare in the context of cyber operations.

A. Preparation of cyber effects

Levels of war such as strategic, operational and tactical levels were introduced in order to enhance decision-making processes and to allow greater efficiency in the execution of tasks. The outcomes of kinetic warfare get more specific when moving from the strategic to the tactical level, i.e. the impact of the outcomes and the responsibilities are more limited. There is no known equivalent simplification in the planning of cyber warfare [13]. It is not even known to what extent cyber operations are achieving their effects [2], this, however, is the objective of this paper: to help nations to find it out.

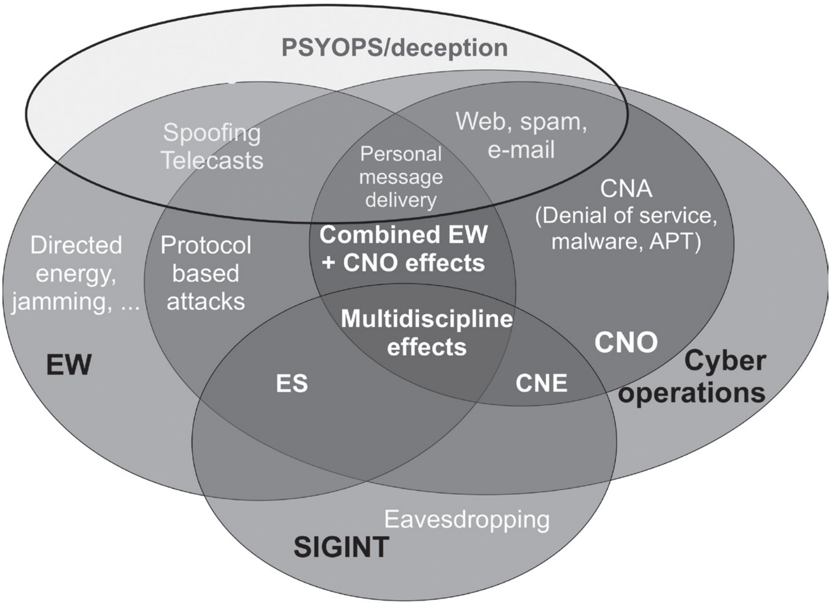
The preparation time of cyber effects can range from very long to almost immediate, depending on the effects to be achieved, the target system, access to information, cyber skills of personnel, etc. Physical distances are often irrelevant.

It is also important for nations to invest in training personnel, e.g. cyber operations training in military academies, exchange programmes of military cadets with technology universities for particular classes, etc. Certainly the areas of Cyber Network Operation, as explained in Figure 2, should have a focus.

It is important for nations to include cyber operations capabilities in their (grand) strategy, but there are not enough resources to prepare and provide cyber effects for all imaginable scenarios. Development of these capabilities may take a considerable amount of time; the focus on and prioritising of which cyber effects are key to an operation and should be performed well in advance of the operation.

Technical aspects, including technical skills, are a critical factor of a cyber operation. A cyber effect is linked to the technical characteristics of the chosen solution. It is often the case that a specific technological solution is most suitable to ensure a specific effect. Therefore, the achievable cyber effects are dependent on available technical know-how. Deciding on the areas in which technical knowledge should be developed has to be planned a long time in advance and incorporated in a strategy. Although not all IT-related capabilities, ranging from electronic warfare, signal intelligence to cyber operations, are subjects of this paper, a national strategy should not only include cyber effects, but all of them. Isaac Porche's [6] overview of the relevant functional areas is provided in Figure 2.

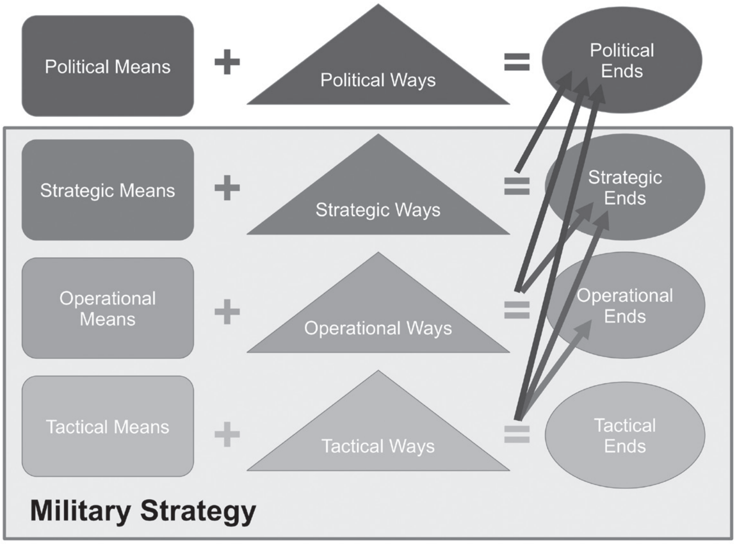
FIGURE 2: FUNCTIONAL VIEW OF CYBER EFFECTS. IT SHOWS THE OVERLAPS AMONG ELECTRONIC WARFARE (EW), SIGNAL INTELLIGENCE (SIGINT) AND CYBER OPERATIONS. COMPUTER NETWORK OPERATIONS (CNO) ENCOMPASSES COMPUTER NETWORK EXPLORATION (CNE) AND COMPUTER NETWORK ATTACK (CNA). ELECTRONIC SUPPORT (ES) ARE TECHNIQUES SUCH AS DIRECTION FINDING OF ELECTROMAGNETIC SOURCES [6].



B. 'Ends' in cyber operations

The use of cyber means and ways at one level of military strategy can potentially impact higher levels of strategy, even reaching the political, especially with regard to cognitive, economic or societal effects. This is not unique to cyber operations, but here this spill-over might be more difficult to predict. Therefore, cyber operations should be authorised by someone responsible for the highest potential level of impact. This is illustrated in Figure 3, based on a graphic by Murat Balci [13], which applies to kinetic warfare. The dotted lines present the spill-over that can happen in cyber operations.

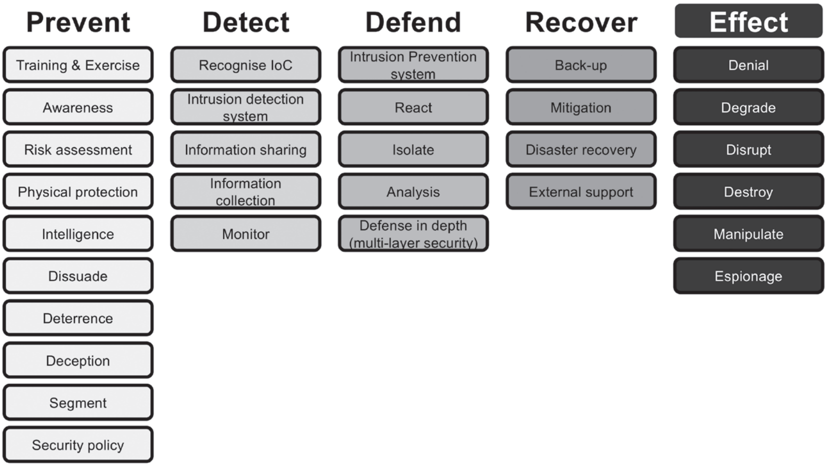
FIGURE 3: WAYS AND MEANS ON TACTICAL, OPERATIONAL, AND STRATEGIC LEVELS CAN RESULT IN ENDS ON A HIGHER LEVEL [13]



Cyber operations are able to destroy, degrade, deny, and disrupt information technology-dependent infrastructures and data. They can be used in espionage and manipulation. Often, they cause cognitive effects with few physical effects [33]. Cyber operations can be used against a specific target (e.g. Stuxnet [30], [34]) or indiscriminately (e.g. Wannacry [35]).

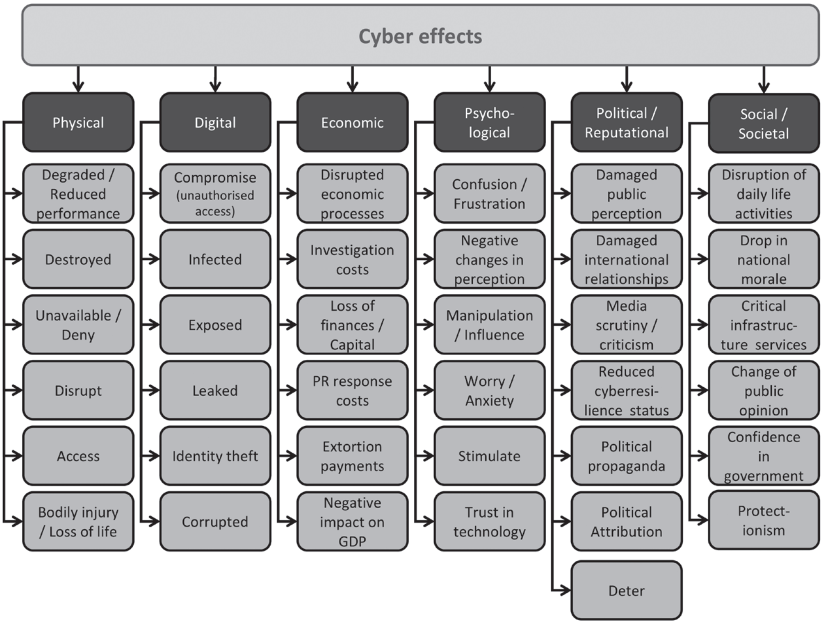
First, from a defensive point of view, there are tasks that should be undertaken or for which training should be provided, in order to deter and to detect adversary cyber operations. There are actions to be taken to defend against cyber operations and to recover from a successful adversary cyberattack, if defence has failed. It is a wise approach to start planning cyber operations only when all of those defensive tasks are taken care of. A non-exhaustive list of tasks in cyberspace in Figure 6 is proposed to the community for discussion. This list is developed from the concepts in NIST's "Framework for Improving Critical Infrastructure Cybersecurity": identify, protect, detect, respond and recover [36]. It is perfectly possible that some tasks are necessary for different purposes or that some tasks are not relevant in some situations.

FIGURE 4: TASKS IN CYBERSPACE [36]



A taxonomy of cyber effects, based on previous work by Agrafiotis [37], is shown in Figure 5. This taxonomy takes into account further effects, such as economic and reputational, while the original taxonomy focused on cyberattacks on commercial enterprises. In this paper, the authors have designed a new taxonomy from the perspective of a nation-state.

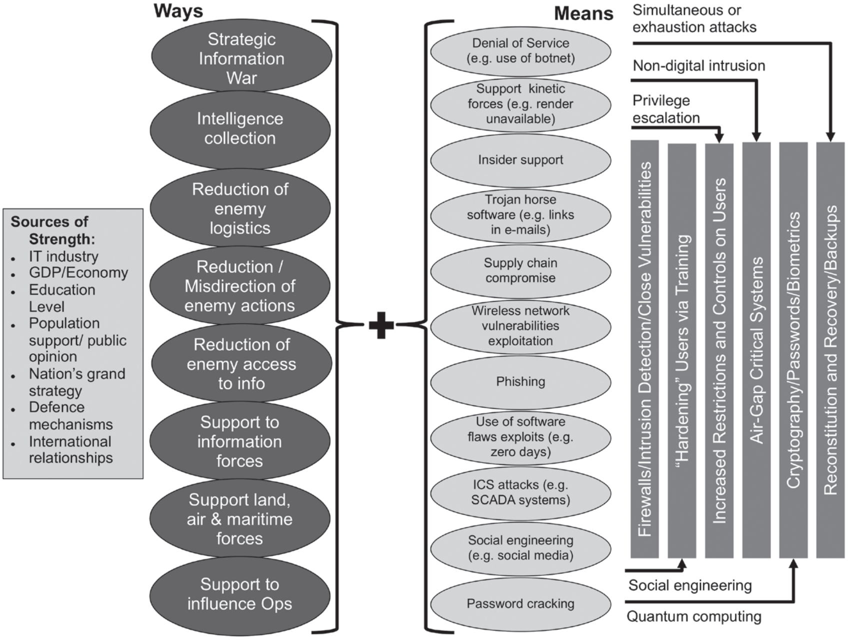
FIGURE 5: ENCOMPASSING TAXONOMY OF CYBER EFFECTS [37]



C. ‘Means’ and ‘Ways’ in cyber operations

Figure 6 proposes a cyberspace superiority model based on the work of William Bryant [38]. The image shows that ways and means can be flexibly mixed in order to achieve the desired outcomes, and that some means are more useful to overcome some typical technical challenges. What adds to the complexity is that they do not get their strength only from military capabilities, but more broadly from the society.

FIGURE 6: CYBERSPACE SUPERIORITY MODEL, WHICH DESCRIBES MEANS, WAYS, AND DEFENSIVE BLOCKS [38]


Ways
Strategic Information War
Intelligence collection
Reduction of enemy logistics
Reduction / Misdirection of enemy actions
Reduction of enemy access to info
Support to information forces
Support land, air & maritime forces
Support to influence Ops
Sources of Strength:
IT industry
GDP/Economy
Education Level
Population support/ public opinion
Nation’s grand strategy
Defence mechanisms
International relationships
+
Means
Denial of Service (e.g. use of botnet)
Support kinetic forces (e.g. render unavailable)
Insider support
Trojan horse software (e.g. links in e-mails)
Supply chain compromise
Wireless network vulnerabilities exploitation
Phishing
Use of software flaws exploits (e.g. zero days)
ICS attacks (e.g. SCADA systems)
Social engineering (e.g. social media)
Password cracking
Simultaneous or exhaustion attacks
Non-digital intrusion
Privilege escalation
Firewalls/Intrusion Detection/Close Vulnerabilities
“Hardening” Users via Training
Increased Restrictions and Controls on Users
Air-Gap Critical Systems
Cryptography/Passwords/Biometrics
Reconstitution and Recovery/Backups
Social engineering
Quantum computing

D. Collaboration in cyber operations

There are a multitude of reasons why different actors would assist each other in achieving a particular end state on a specific target, and this has not changed with the emergence of cyberspace. There are huge differences in nations’ capabilities to develop and launch cyber operations, so it makes sense that some state actors are willing to offer cyber effects to other nations or organisations. The sharing of technical and operational details of cyber operations is very sensitive, which makes collaboration difficult. To some extent, the use of cyber operations could be compared with the use of Special Forces: there is an agreement on which effects one wants to achieve, but very little or no information will be shared about how this will be, or has been, executed.

Communities are built to share information about defending networks and computer systems. Most of them are public fora that share known vulnerabilities. They exist in the public domain, like MISP (NATO’s malware information sharing platform), and in the private sector, where most software security companies post discovered vulnerabilities on their websites. In the open source community there are fora for sharing information, as well as initiatives like Metasploit [39], which is a framework that includes known vulnerabilities for the purposes of software penetration testing. The public sharing of this kind of information, even information gained from offensive penetration testing, is done from a defensive point of view.

In cyber warfare some cyber effects are usable only once. For example, if a cyber effect is based on the use of a zero-day vulnerability, sharing this information could render this exploit unusable if it were leaked or used elsewhere.

Coalition partners must be informed about capabilities. This is needed in order to understand expected cyber effects, to estimate both the probability of success, the expected collateral damage, and it creates trust. The aim of the exchange of additional information is not to replace any existing targeting procedures, but rather to enhance the ‘capabilities analysis’ aspect for cyber effects. A more legal approach to targeting in cyberspace can be found in ‘Joint and combined targeting: system and process’ [40].

Where possible one should express the desired effect by using existing terminology from kinetic warfare. Terminology describing effects, such as ‘deny’, ‘degrade’, ‘disrupt’, and ‘destroy’ can be used for cyber effects. Some additional effects, such as those mentioned in Figure 5, are more specific to cyber effects. This paper endorses the use, as much as possible, of existing terminology and procedures, because this integrates cyber effects more smoothly into the existing military decision-making process and facilitates the comparison of cyber effects with other means of achieving an objective.

4. RECOMMENDATIONS AND FUTURE WORK

A. Measuring and predicting cyber effects

1. Cyber effects can easily trigger outcomes, wanted or unwanted, on a strategic or a political level. Ensure that the use of cyber operations is authorised by the strategic level that aligns with the estimated ends of the cyber effect. This implies that the Rules of Engagement (RoE) delegation for cyber operations should be kept at a corresponding level. This diverges

from traditional kinetic warfare, where responsibility is delegated and use of force is limited in cascade, by using specific rules of engagement for each decision level.

2. A solid understanding of the expected outcome of the first-, second-, and third-order cyber effects will facilitate better decision-making as to whether a cyber effect is the best course of action to reach a specific goal, and will increase the effectiveness of its use.
3. Define the desired cyber effects with the fewest technical terms and use existing terminology whenever possible. A good understanding of the strengths and weaknesses of the technical possibilities of cyber effects is crucial for the cyber advisor, who should be capable of translating into non-technical language. Appropriate visualisation tools should be put in place in order to have more situational awareness; this will help with the battlefield damage assessment caused by a cyber effect.

B. Achieving cyber effects

1. The cyber operation will be one possible course of action for a commander. A cyber operation is not a 'silver bullet' that will provide a solution when traditional means are not able to achieve a desired end state. On the other hand, if a cyber or hybrid operation has been integrated into the planning process from the beginning, it could be the best option a commander has for executing a specific task or achieving a desired end state.
2. Before considering investment in cyber operations capabilities, the ideal situation is to verify that the mission's IT infrastructure is not vulnerable to cyber exploits, and that mission assurance is guaranteed from a cyber perspective. Therefore, as explained in Figure 6, if feasible, all cyber tasks in support of prevention, detection, defence, and recovery should be covered before enabling cyber operations, but everything depends on the risk assessment and the capabilities of the adversary.
3. Guaranteeing mission assurance from a cyber perspective implies that the mission's IT infrastructure is not vulnerable to the developed cyber exploits, but also to a possible counter cyber effect originating from the target as a response to the initial cyber operation, also called a 'hack-back'.
4. On a national political level, having a long-term political vision of what type of cyber capability should be developed is key. There are not enough human resources nor financial means to build every possible cyber capability in advance. On a political level, the following questions should be addressed: "What is the main focus of the cyber capabilities?" and "How much effort will be invested in research, and for which types of cyber capability?"

5. When cyber effects are needed, there could be too little time for development if they have not been prepared and trained for in advance. Creating high-impact, targeted, cyber capability with limited collateral damage requires substantial preparation time.
6. Ensure that a cyber advisor is present at every level of decision-making. Cyber operations are technical in nature and it is a challenge to translate those technical aspects into operational language in terms of 'means', 'ways' and 'ends'.
7. Make sure that the cyber domain is involved in the planning process as early as possible, from the beginning of the planning of every campaign. This will optimise the outcome of cyber effects.

C. Future work

1. Until now there has been little input from the legal community with regard to collateral damage in cyberspace. Legal specialists should develop this topic in more detail.
2. If a cyber effect will be delivered by a supporting nation, there is a need to streamline the coordination and exchange of information. Nations delivering voluntary sovereign contributions need to receive information from the mission commander, and the mission commander needs feedback from the supporting nation in order to integrate this in the planning process. Information sharing about this among allies is not yet well developed. A framework should be developed that defines the essential elements of information to be exchanged, and describes how to do this. Due to the sensitive nature of the technical details of cyber capabilities, more focus should be put on ends and effects rather than on technical aspects, without neglecting the specificities of a cyber effect. The level of detail of the information coming from the national sovereign contribution to the mission must allow the mission commander to be confident that the desired end goals will be achieved, that mission assurance is not compromised, and that collateral damage is under control.

5. CONCLUSIONS

Cyber operations are advisable when the effects are planned well in advance, and when one's own systems are well protected. Achieving cyber effects should take into account that it is difficult to estimate the spill-over to other levels of warfare. Support from one nation to another or to a coalition in order to achieve cyber effects sounds promising, but publicly known procedures how to achieve this do not exist yet.

Whoever can influence the portion of cyberspace used by the adversary has the potential to control the adversary. Cyber effects can, in specific circumstances, be the most effective tool to disrupt, degrade, corrupt, influence, etc. an adversary's ability to conduct military operations. The ability to accurately estimate the impact of cyber effects is currently limited. Just as in kinetic warfare, estimations and measurements of outcomes of cyber effects are essential in planning operations because they allow decision-makers to optimise the outcome and to limit the unwanted effects or collateral damage.

REFERENCES

[1] R. C. Parks and D. P. Duggan, "Principles of Cyberwarfare," in *Workshop on Information Assurance and Security*, 2001, pp. 122–125 on page 122.

[2] S. Musman, A. Temin, M. Tanner, D. Fox, and B. Pridemore, "Evaluating the Impact of Cyber Attacks on Missions", MITRE Corp., 2010.

[3] J. Döge, "Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime" *Arch. des Völkerrechts*, vol. 48, no. 4, pp. 486–501, 2011on page 488.

[4] S. A. Hildreth, "CRS Report to Congress: Cyberwarfare" 2001 in footnote 3. [Online]. Available: https://fas.org/sgp/crs/intel/RL30735.pdf. [Accessed: 19-Feb-2019].

[5] O. A. Hathaway et al., "The law of cyber-attack" *Yale Law Sch. Fac. Scholarsh. Ser.*, pp. 817–886, Jan. 2012 on page 883.

[6] I. R. Porche et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World" RAND Corporation, 2013 on page 15.

[7] K.V. Clausewitz, *On war*. Translated to English in 1943 by Jolles, on page 16.

[8] US Air Force, US Air Force doctrine, 2015 in Vol 1 Basic Doctrine. [Online]. Available: https://www.doctrine.af.mil/Core-Doctrine/Vol-1-Basic-Doctrine/. [Accessed: 19-Feb-2019].

[9] The European Centre of Excellence for Countering Hybrid Threats, "Blog: Hybrid threats – what are we talking about?" www.hybridcoe.fi, 2017. [Online]. Available: https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/. [Accessed: 19-Feb-2019].

[10] M. C. Libicki, "The Convergence of Information Warfare" *Strateg. Stud. Q.*, vol. 11, no. 1, pp. 49–65, 2017 on page 54.

[11] C. Cadwalladr and E. Graham-Harrison, "How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool" *The Guardian*, International edition, 17-Mar-2018.

[12] Mandiant, "M-TRENDS2018" 2018 in "2017 by the numbers", "Dwell time". [Online]. Available: https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf. [Accessed: 19-Feb-2019].

[13] M. Balci, M. Canan, and G. Kucukkaya, "Defining military levels for cyber warfare by using components of strategy: ends, ways, and means" in 21st ICCRTS "C2 in a Complex Connected Battlespace"'," 2016, pp. 1–13 on page 5.

[14] Council on Foreign Relations, "NotPetya" 2017. [Online]. Available: https://www.cfr.org/interactive/cyber-operations/search?keys=not+petya. [Accessed: 19-Feb-2019].

[15] R. A. Martino, "Leveraging traditional battle damage assessment procedures to measure effects from a computer network attack" Air Force Institute of Technology, 2011 on page iv.

[16] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework" in *5th International Conference on Cyber Conflict (CyCon)*, 2013.

[17] B. K. Mishra and H. Saini, "Cyber Attack Classification using Game Theoretic Weighted Metrics Approach" World Appl. Sci. J., vol. 7, no. *Special Issue of Computer & IT*, pp. 206–215, 2009.

[18] B. Edwards, A. Furnas, S. Forrest, and R. Axelrod, "Strategic aspects of cyberattack, attribution, and blame" *Proc. Natl. Acad. Sci.*, vol. 114, no. 11, pp. 2825–2830, 2017.

[19] M. Jones, G. Kotsalis, and J. S. Shamma, "Cyber-attack forecast modeling and complexity reduction using a game-theoretic framework" in *Control of Cyber-Physical Systems*, Springer, 2013, pp. 65–84.

[20] F. Yıldız, "Modeling the effects of cyber operations on kinetic battles" *Engineering*, pp. 32–37, 2014.

[21] P. Johnson, J. Ullberg, M. Buschle, U. Franke, and K. Shahzad, "An architecture modeling framework for probabilistic prediction" *Inf. Syst. E-bus. Manag.*, vol. 12, no. 4, pp. 595–622, Nov. 2014.

[22] W. S. Powell, "Methodology for Cyber Effects Prediction" in Black Hat USA, 2010.

[23] D. E. Denning, "Assessing Cyber War" in *Assessing War*, L. J. Blanken, H. Rothstein, and J. J. Lepore, Eds. Georgetown University Press, 2015, pp. 266–284.

[24] A. Phillips, "The asymmetric nature of cyber warfare" *USNI News*, Feb-2013. [Online]. Available: https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare#more-785. [Accessed: 23-Feb-2019].

[25] S. Mele, "Cyber-Weapons: Legal and Strategic Aspects (Version 2.0)" *Instituto Italiano Di Studi Strategici,* 2013 on page 13. [Online]. Available: https://papers.ssrn.com/sol3 /papers.cfm?abstract_id=2518212. [Accessed: 19-Feb-2019].

[26] B. J. Egan, "International Law and Stability in Cyberspace" *Berkeley J. Int. Law*, vol. 35, no. 1, pp. 169–181, 2017.

[27] DoD Joint Chiefs of Staff, No-strike and the collateral damage estimation methodology. U.S.A., 2012.

[28] S. Romanosky and Z. Goldman, "Cyber Collateral Damage," *Procedia Comput. Sci*., vol. 95, pp. 10–17, 2016.

[29] M. N. Schmitt, *Tallinn Manual 2.0* on the international law applicable to cyber operations. 2017 on page 475.

[30] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier" 2011.

[31] M. Daniel, "Heartbleed: Understanding when we disclose cyber vulnerabilities" White House blog, April, 2014. [Online]. Available: https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities. [Accessed: 23-Feb-2019].

[32] D. Laich, "Ends = Ways + Means" mglaich, 2010. [Online]. Available: http://mglaich.blogspot.com/2010/07/ends-ways-means.html. [Accessed: 23-Feb-2019].

[33] S. Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence" *Commun. ACM*, vol. 54, no. 8, pp. 132–140, Aug. 2011.

[34] J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare" *Secur. Stud*., vol. 22, no. 3, pp. 365–404, 2013.

[35] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017" *Int. J. Adv. Res. Comput. Sci*., vol. 8, no. 5, pp. 1938–1940, 2017.

[36] NIST (National Institute of Standards and Technology), "Framework for improving critical infrastructure cybersecurity" Feb. 2014 on page 19.

[37] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate" *J. Cybersecurity*, pp. 1–15, 2018 on page 8.

[38] W. D. Bryant, "Cyberspace Superiority: A Conceptual Model," *Air Sp. Power J*., pp. 25–44, 2013 page 37.

[39] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies" *CINTI 2014 - 15th IEEE Int. Symp. Comput. Intell. Informatics, Proc*., pp. 237–242, 2014.

[40] M. N. Schmitt, J. Biller, S. C. Fahey, D. Goddard, and C. Highfill, "Joint and combined targeting: system and process" 2016 pages 13 to 19. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830229. [Accessed: 19-Feb-2019].