An Anticipatory Ethical Analysis of Offensive Cyberspace Operations

Gazmend Huskaj¹² and Richard L. Wilson³⁴
¹Swedish Defence University, Stockholm, Sweden
²University of Skövde, Sweden
³Towson University, USA
⁴Senior Research Scholar, Hoffberger Center for Professional Ethics, University of Baltimore, USA

gazmend.huskaj@fhs.se
wilson@towson.edu
DOI: 10.34190/ICCWS.20.054

Abstract: This article presents the ethical issues using offensive cyberspace operations. Previously enshrouded in secrecy, and now becoming the new norm, countries are using offensive cyberspace operations to achieve their strategic interests. Russia has conducted multiple offensive operations targeting Estonia, Georgia and the Ukraine; Hamas has targeted Israeli targets; and Iran has been targeting U.S. targets. The response to these operations has varied; Estonia and Georgia struggled with the attacks and were unable to respond while Ukraine tried to respond but the response was inefficient. Israel’s response on Hamas offensive operations was an air strike on a building with Hamas Cyber-operatives. Iran shot down a U.S. Drone over the Strait of Hormuz, and the U.S. initially intended to respond with kinetic capabilities in the form of missile strikes. However, in the last minute, the U.S. chose to respond with offensive cyberspace operations targeting the Iranian missile systems. This last-minute change of response choosing between kinetic or cyber capabilities shows a need to further investigate how offensive cyberspace operations can be used against which targets from an ethical perspective. This article applies anticipatory ethical analysis on U.S. offensive operations in the “Global Hawk”-case when Iran shot down a U.S. drone over the Strait of Hormuz. Anticipatory ethical analysis looks at emerging technologies and their potential consequences. Offensive cyberspace operations present a range of possibilities, which include lowering the risk of harm to cyber operatives’ lives belonging to the responding nation. However, a response can also be kinetic. Therefore, the analysis of the “Global Hawk”-case is compared with the Israeli-air strike of the building of Hamas Cyber-operatives. The authors argue that applying anticipatory ethical analysis on offensive operations and kinetic operations assist decision makers in choosing response actions to re-establish deterrence through the use of offensive cyberspace operations.

Keywords: Offensive Cyberspace Operations, Anticipatory Ethics, Deterrence, Response, Kinetic.

1. Introduction

This article presents the ethical issues related to using offensive cyberspace operations. The analysis is a case study and anticipatory ethical analysis of offensive cyberspace operations. Previously enshrouded in secrecy, and now becoming the new norm, countries are using them to achieve their strategic interests. Russia has conducted offensive operations targeting Estonia, Georgia and the Ukraine; Hamas was targeting Israeli targets; and Iran has been targeting U.S. targets. The response has varied; Estonia and Georgia struggled with the attacks and were unable to respond while Ukraine tried to respond but it was inefficient. Israel’s response on Hamas offensive operations was an air strike on a building with Hamas Cyber-operatives.

These cases also show how nation states are integrating offensive operations with traditional military capabilities, and consider them as an addition tool to demonstrate power. In addition to the demonstration of power, they are also used to increase the deterrence posture of nation states. However, deterrence works only if the deterrent is able to get the threat of retaliation into the threat actors mindset. To achieve this, the deterrent is required to have a base where power is gained from, to signal that the deterrent will use capabilities (means) to retaliate, the amount of capabilities (means), and the scope of potential targets (Huskaj & Moradian, 2018). However, this is no guarantee the deterrent will succeed in getting the threat of retaliation into the threat actors mindset unless employing actual capabilities. These capabilities may fall into the realm of soft power (e.g. sanctions); into the realm of hard power (e.g. kinetic or non-kinetic strikes), or a combination of both. Therefore, the deterrent must also have the will to use capabilities. Schelling (1966) best describes will by taking the example of inmates in mental institutions who threaten the attendants “that they may slit their own veins or light their clothes on fire if they don’t have it their way. I understand that they sometimes have their ways” (Schelling, 1966: 37-38). This description of deterrence capabilities may not be required for the use of offensive cyberspace operations.
Real-world cases until now have revealed offensive operations just below the threshold of kinetic warfare. The tools, e.g. a computer, an internet-connection, and operators, are not expensive compared to the cost of traditional military capabilities. However, deep technological knowledge is required by the operators to be able to penetrate adversary systems. This particular expertise takes time to develop because of the many aspects of internet worked information systems, related hardware and software, and their inherent security controls. Therefore, state actors can either recruit and train people to become cyber operators, or use asymmetric means by employing various forms of state-sponsored actors which may fall into categories like organised crime and ‘patriotic-hackers.’ The methods used for offensive operations use include “provid[ing] data to a program running on that system that causes it to act on behalf of the attacker” (O’Leary, 2019, p.51).

One concrete example is the 1988-Morris worm. It “attacked vulnerable services including fingerd and sendmail [and] when it attacked fingerd, it sent a 536-byte request to C code using gets() that provided a buffer with only 512 bytes of space; the resulting overflow allowed the worm’s code to execute on the target” (O’Leary, 2019, p.51). This is what is also known as a ‘buffer overflow.’ Much has happened since 1988 and the attack surface has increased.

2. The MQ-4 Triton-case

This section describes the events prior and after the downing of a US military drone, the MQ-4 Triton, by the Iranians. This is also the main case focused on in this analysis.

On 13 June, 2019, the Iranian Revolutionary Guard used limpet mines targeting Norwegian and Japanese tankers in the Gulf of Oman (Schmitt, 2019). The event triggering the attacks was allegedly the result of the US withdrawing from the multilateral nuclear agreement, and re-imposing sanctions on energy, shipping, financial sectors and the petrochemical sector (AP, 2019; BBC, 2019). These sanctions are also known as the Trump administration’s “maximum pressure campaign” (McLaughlin et al., 2019). The sanctions have “led to shortages of imported goods and products that are made with raw materials from abroad, most notably babies’ nappies [and] the plunging value of the rial has also affected the cost of locally produced staples such as meat and eggs” (BBC, 2019).

U.S. officials threatened to respond “if U.S. interests in the region were harmed. Then, on Thursday, the Iranians shot down a $240 million U.S. military drone” (McLaughlin et al., 2019). The drone, a MQ-4 Triton, is the Navy version of the Global Hawk. The Global Hawk provides intelligence, surveillance and reconnaissance (ISR) capabilities, and the Navy version “performs a ‘Broad Area Maritime Surveillance (BAMS-D)’ ISR mission” (Schmitt, 2019). The Trump administration intended a kinetic response, however, the kinetic option was ruled out when President Trump “learned 150 Iranians might die” (McLaughlin et al., 2019).

On 20 June, 2019, U.S. Cyber Command conducted offensive cyberspace operations targeting a database used by “an Iranian spy group ... to track and target military and civilian ships passing through the economically important Strait of Hormuz” (McLaughlin et al., 2019). Additional reporting notes that Iranian command and control systems for “rocket and missile systems” were targeted (BBC, 2019). Final reporting notes an operation to “disable and degrade [the] networked communications [of] Kata’ib Hezbollah” (Starr, 2019). Kata’ib Hezbollah, a Shia militia group, is sponsored by Iran to conduct attacks on U.S. targets and their allies (Starr, 2019).

3. Offensive Cyberspace Operations

This section describes the process for offensive operations. For the purposes of this paper, the process for offensive operations is based on Joint Publication 3-12, Cyberspace Operations. Offensive cyberspace operations are defined as a sequence of planned actions executed by an organised group of people with a defined purpose in and through hardware and software which are used to create, process, store, retrieve and disseminate information in different types of interconnected networks that build a large, global network, built and used by a wide variety of people. The offensive aspect includes methods to affect an adversary’s target system’s confidentiality, integrity and/or availability. These targets include “weapon systems, C2 processes, logistics nodes, high-value targets” (p.II-5).

Prior execution, authority is “derived from DOD policy memorandum, directive, or instruction [which] authorises a military order” (p.II-2). It is the “intent or objective of the issuing authority” (p.II-2) that results in
the categorisation of an operation as offensive or defensive. Next, intelligence collection and targeting is done, followed by coordination and deconfliction, and execution and assessment (p.II-11). The purpose with offensive actions is to “create noticeable denial effects” (p.II-7). Denial effects include degrade, disrupt and destroy.

“1. Degrade. To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified.

2. Disrupt. To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent.

3. Destroy. To completely and irreparably deny access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.” Source: (ICS, 2018, p.II-7).

The offensive methods to generate denial effects are depicted in Table 1.

**Table 1: Offensive methods**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Overflow Tactics and Techniques</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Rootkits</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Redirection and Triggering</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Redirection, Triggering, and Exfiltration</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tunneling</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Collection/Exfiltration</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web Exploitation</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Persistent Access</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Man-in-the-Middle</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(Distributed) Denial of Service</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Obfuscation</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Once inside an adversary’s targeted system, actions to degrade, disrupt or destroy are performed. ‘Operation Glowing Symphony’ illustrates this: login into adversary accounts, delete files, folders, change passwords of adversary accounts, and buy domain names (Temple-Raston, 2019).

**4. Understanding Ethics**

This section describes the ethical issues with offensive cyberspace operations. Offensive cyberspace operations include efforts to generate deny, degrade and destroy effects. Deceive and manipulate effects may also be used for offensive purposes. For this paper however, these effects are defined to affect the cognitive abilities of the user, and therefore not covered. Furrow (2005) identifies the focus of ethical analysis as involving a series of factors. Furrow (2005) states that ethics is related to evaluating actions and actions are performed by those capable of being moral agents. He says, “When we evaluate an action, we can focus on various dimensions of the action. We can evaluate the person who is acting, the intention or motive of the person acting, the nature of the act itself, or the consequences.” (Furrow, 2005, p.44).

Two key points can be made from Furrow’s distinctions. The first point is that ethical issues related to deny, degrade and destroy are based upon the idea that those who generate deny, degrade and destroy effects are actions, and these actions are an extension of what a person intends. The second is that the actions to generate deny, degrade and destroy effects are capable of being evaluated based upon the intentions and actions of the people engaged in those activities. Applying Furrow’s (2005) distinctions to deny, degrade and destroy leads us to three possible levels of ethics evaluation. First, the actions of a person generating deny, degrade and destroy effects. Second, the intentions of a person’s actions to generate deny, degrade and destroy effects. Third, the nature of the act, or the consequences of the actions intended by the person(s) generating deny, degrade and destroy effects.
The actions of agents generating deny, degrade and destroy effects are subject to ethical evaluation based on the actions of the person(s) conducting offensive operations, the intentions or motives of that person, and the consequences produced by deny, degrade and destroy effects. According to Furrow (2005), it is ultimately the person or persons who are conducting offensive operations that are subject to moral evaluation. Identifying the ethical issues with deny, degrade and destroy, requires asking four questions: 1) what actions are performed when generating deny, degrade and destroy effects; 2) what is the character of the person(s) generating those effects; 3) what are the intentions of those generating deny, degrade and destroy effects; and 4) what are the consequences of deny, degrade and destroy effects.

The ethical issues with emerging technologies are the result of how these technologies are used to generate deny, degrade and destroy effects. The purpose of generating these effects is to achieve a tactical, operational or strategic goal by the person or persons. There is the controller of deny, degrade and destroy, and who and what is affected by the activities of deny, degrade and destroy. The intention of the person or persons of deny, degrade and destroy involves instrumental reasoning and establishing a purpose for the use of deny, degrade and destroy, as well as a goal (such as denying an adversary’s ability to plan and execute operations to capture oil tankers). Next are the adversary’s forces affected by the purpose of deny, degrade and destroy which involves the technical issue of loss of information to plan, prepare and execute operations; the use of weapon systems to pose a threat; or the use of communication systems to coordinate, and command and control forces. The interaction between the technical use of deny, degrade and destroy by the person or persons to affect an adversary’s decision making, command and control, and the employment of weapon systems, and the technical effect of deny, degrade and destroy as it affects information systems holding information for decision making, command and control, or steering weapon systems, is where ethical issues with deny, degrade and destroy arise. Given additional space a preliminary ethical analysis could be developed by applying standard ethical principles. These standard ethical principles would be applied to how the intentions, actions, and outcomes produced by the person(s) generating deny, degrade and destroys affect the adversary.

5. Stakeholders

This section covers the stakeholders in the case. Stakeholders are defined as those who are affected by the actions of Iran, and the follow-up to these actions which is a response by offensive cyberspace operations. The ethical issues emerge due to the conflict between these stakeholders. The same accounts for the social issues. Stakeholders are divided into primary and secondary. Primary are those directly affected by Iranian actions and the follow-up response offensive operation. Secondary are those indirectly affected by the conflict.

Primary stakeholders. The Iranian Government (IG) and the Iranian Revolutionary Guard (IRG) - these parties have the intent and capability to conduct attacks on oil tankers in the Gulf of Oman, and Strait of Hormuz. They are responsible for seizing British-linked oil tankers and using limpet mines on Norwegian and Japanese-owned oil tankers. They also shot down the Navy’s MQ-4C “Triton” using “a variant of its Raad surface-to-air missile (SAM) system [known as the] 3rd Khordad transporter erector launcher and radar” (O’Connor, 2019).

Crew of oil tankers - these parties are directly affected by the threat actions of the IG and IRG because of the limpet mines used on the tankers, forcing the crew to leave their tankers, but also by seizing the British-linked oil tankers (Borger, 2019).

The U.S. Navy - this party was directly affected when its MQ-4C “Triton” was shot down while conducting surveillance (Neuman, 2019).

Secondary stakeholders include Japan, Norway, Sweden, the U.K., and the U.S. These parties either own the oil tankers and/or have interests in the area to make sure the operations of the tankers are not disrupted.

The public (consumers of oil, gas and gasoline). These are the citizens of the world that use, for example, gasoline to fuel their vehicles.

6. Technical / professional problems

The technical issues related to the surface-to-air-missile shooting down the Triton, the technical issues related to the limpet mines, and the initial kinetic response by the Trump-administration, are deemed as self-
explanatory and will not be covered here. What is covered however are the technical issues related to offensive cyberspace operations. Denial effects, i.e. Degrade, disrupt and destroy, have already been referred to above. In addition, offensive methods are mentioned in Table 1. To get an idea of an attack vector, offensive methods are clustered into software applications, network, web applications, and the users of the system under attack.

6.1 Software applications.
Buffer overflow tactics and techniques involve “overwriting of memory fragments of the process, which should have never been modified intentionally or unintentionally” (OWASP, 2014). A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code (OWASP, 2016).

Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed, and such elevation or changes should have been prevented by the application. This is usually caused by a flaw in the application. The result is that the application performs actions with more privileges than those intended by the developer or system administrator. (OWASP, 2017).

Rootkits. A rootkit is a set of malicious applications, which allows an adversary to access privileged software areas on a machine while at the same time hiding its presence. Note, by machine, we mean the full spectrum of IT systems from smartphones to Industrial Control Systems. (ENISA, n.d.)

Persistent access. “During a Red Team engagement, a lot of time and effort is spent gaining initial access to an organization, so it is vital that the access is maintained in a reliable manner.” (Hawkins, 2019).

Obfuscation. “The code obfuscation is a mechanism for hiding the original algorithm, data structures or the logic of the code, or to harden or protect the code (which is considered as intellectual property of the software writer) from the unauthorized reverse engineering process. In general, code obfuscation involves hiding a program’s implementation details from an adversary, i.e. transforming the program into a semantically equivalent (same computational effect) program, which is much harder to understand for an attacker.” (Behera & Bharskari, 2015).

6.2 Network
Redirection, triggering and exfiltration. “This vulnerability occurs when an application accepts untrusted input that contains an URL value without sanitizing it. This URL value could cause the web application to redirect the user to another page as, for example, a malicious page controlled by the attacker. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Since the redirection is originated by the real application, the phishing attempts may have a more trustworthy appearance.” (OWASP, 2014).

Triggering is about triggering an error in a database, or an unhandled error condition in an application. Triggering an error in a database can result in displaying the name of the database. This facilities the information collection phase to further exploit vulnerabilities, such as a SQL-injection attack (OWASP, 2014). Triggering unhandled error conditions in an application can lead to a denial of service attack, “because they reveal a lot of information about databases, bugs, and other technological components directly linked with web applications.” (OWASP, 2014).

Tunneling involves using various techniques to bypass security controls like a firewall and/or restricted networks (Mis, 2018; Fortuna, 2019). These methods are used for data collection/exfiltration. Additional exfiltration methods include to compress and encrypt data (MITRE, n.d.).

Collection. “Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary’s objectives.” (MITRE, n.d.)
Man-in-the-middle. This type of attack can either eavesdrop the communication between clients, and/or impersonate a real client (Asokan et al., 2002). The “attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.” (OWASP, 2015).

(Distributed) Denial of Service ((D)DoS). Two methods of (D)DoS exist: on the network level and the application level (OWASP, 2010). The purpose of this attack is to degrade or disrupt a web application or server.

6.3 Web applications/exploitation
This attack is about collecting information on websites, web applications, and exploiting the identified vulnerabilities. The purpose could be to buy products at a cheaper price, damaging the owner’s reputation, or stealing sensitive information (Tran, n.d.).

6.4 The user
Social engineering. “Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action.” (MITRE, n.d.). This method is supported by collecting information and “identifying key personnel or individuals with critical accesses in order to best approach a target for attack.”

7. The social consequences of offensive cyberspace operations
This section describes the social consequences of offensive cyberspace operations. Cyberspace has led to increased interconnectedness enabling people and companies leading to the exchange of ideas, information and also conducting business in previously unthought about ways. This has also enabled threat actors to conduct attacks, steal information to bridge the technological gap, but also to take information systems and their information for ransom. These threats have resulted in nation states developing organisations to conduct both defensive and offensive operations. The purpose with defensive operations is to protect infrastructure, systems and information. The purpose with offensive operations have already been mentioned. Offensive methods enable collection to generate an understanding about the adversary, which in turn also supports planning. Furthermore, collection can also assist in identifying the characteristics of cyberspace capabilities for gaining access, maintain persistence, to exfiltrate data, but also to generate degrade, disrupt and destroy effects.

A number of ethical issues arise when developing capabilities to generate degrade, disrupt and destroy effects in information computer systems (ICCs). The first issue is the likelihood these capabilities may spread beyond their intended target(s), resulting in cascading effects. The best known case illustrating this is WannaCry. WannaCry is attributed to a North Korean threat actor known as the Lazarus Group (Fruhlinger, 2018). WannaCry is a type of ransomware which encrypts the information stored in an information systems and demands a ransom from the user(s) to decrypt it. The malicious code had wormlike capabilities and used a flaw in the Server Message Block (SMB) protocol to spread in the network. The code to exploit the flaw was known as EternalBlue (Fruhlinger, 2018). When WannaCry was used by the Lazarus Group, it resulted in cascading effects affecting many civilian targets, including the British National Health Service (NHS). Offensive capabilities cannot have flaws like this spreading beyond their intended target(s) affecting civilian infrastructure. Therefore, capabilities that generate degrade, disrupt and destroy effects must be tested and evaluated prior live fire.

Two types of capabilities exist: those under the constant control of an operator, and those that resemble a “fire and forget”-solution. Capabilities under constant control of an operator are required to generate access. Once access is generated, it is important to create persistence to maintain access reliably because an exploit that was used to generate that access could be patched the next day. One way to maintain access is using a rootkit. It is important to channel commands communicated to the adversary target to avoid triggering various security protocols. Once inside the target, collecting information is done to further increase knowledge, but also to achieve objectives in the target system. Finally, when ‘GO’ is given, the operators conduct the necessary actions like deleting files, folders, changing passwords of adversary accounts, and buying domain names. Additional actions could include acting to encrypt or destroy online backups, and to wipe the adversary’s hard drives in all targets simultaneously.

However, additional intelligence is required to distinguish whether the targets are on their own systems, or if they are in ‘the cloud.’ As noted before, offensive operations should not affect civilian infrastructure. Therefore, if the adversary target is in the cloud and to intentionally reduce the risk of affecting civilian
infrastructure, information about what virtual machines are running, how they are compartmentalised, and the type of hypervisor, is required prior conducting offensive actions.

The second type of offensive operation resembling a “fire and forget”-solution has one additional requirement: the consequences of that code ending up in adversarial hands. The consequence in such a scenario could be the adversary reverse-engineering the code, tampering with it, and then firing it back. This kind of tampering could be enough to change the signature of the capability, rendering detection capabilities useless. This is what is alleged about EternalBlue exploiting the flaw in the SMB protocol: a nation state developed it and it was “stolen by a hacking group known as the Shadow Brokers, who released it obfuscated in a seemingly political Medium post on April 8, 2017” (Fruhlinger, 2018).

8. Anticipatory Ethical Analysis

According to James Rachel’s (Rachel’s, James. The Elements of Moral Philosophy), “Morality is, at the very least, the effort to guide one’s conduct by reason – that is, to do what there is the bests reasons for doing – while giving equal weight to the interests of each individual affected by one’s action.” This conception of morality gives a fundamental picture of what it means to be a conscientious moral agent. A moral agent “is someone who is concerned impartially with the interests of everyone affected by what he or she does; who carefully sifts facts and examines their implications; who accepts principles of conduct only after scrutinizing them to make sure they are justified; who is willing to ‘listen to reason’ even when it means revising prior convictions; and who, finally, is willing to act on these deliberations.”

Referring to Furrow (2005) above, the actions of deny, degrade and destroy are subject to ethical evaluation. This evaluation is based on the actions of the person(s) controlling the technologies that generate deny, degrade and destroy effects. The intentions of person(s) and the consequences generated by their offensive effects can be accessed. Cascading effects like those of WannaCry have negative consequences on all affected targets and risk harming humans, but also affecting business and nation states’ economic security. It is these people who generate deny, degrade and destroy effects on an IICS system are subject to moral evaluation (Furrow, 2005).

Identifying potential problems like WannaCry and attempting to anticipate ethical problems that may emerge is important for policy development. Therefore, a set of five rules have been developed by a community of scholars to help guide thoughts about computing artefacts. All capabilities that generate deny, degrade and destroy effects are computer artefacts. The first rule states, “The people who design, develop, or deploy a computing artefact are morally responsible for that artefact, and for the foreseeable effects of that artefact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artefact as part of a sociotechnical system.” The application of this rule would be that software developers developing cyber capabilities need to test and evaluate them in a safe environment. This would apply to the WannaCry virus.

The second rule of the five states, “The shared responsibility of computing artefacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying or using the artefact. Instead, a person’s responsibility includes being answerable for the behaviours of the artefact and for the artefact’s effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.” This second rule would state that organisations, state-sponsored groups, or nation state organisations, are responsible for the actions of the operators and the effects generated by the capabilities.

The fifth rule of the five rules is, “People who design, develop, deploy, promote, or evaluate a computing artefact should not explicitly or implicitly deceive users about the artefact or its foreseeable effects, or about the sociotechnical systems in which the artefact is embedded.” It would be difficult for a nation state conducting responsible offensive operations to adhere to this rule. This rule is in direct conflict with operational security. Operational security is about keeping all actions and activities related to a planned and ongoing operation secret. Breach of operational security leads to results in the adversary to patch and apply additional security control on the intended targets.
9. Anticipatory Ethical Recommendations/Policy

Recommendations are made based on the conclusions of the ethical analysis. The conclusions of the ethical analysis form the basis of an anticipatory ethical analysis and policy recommendations. It is anticipated that organisations, state-supported groups, and nation states will conduct offensive operations. Those conducting offensive operations can conduct them either responsibly or irresponsibility. Responsible operations include response operations in the downing of the Triton-case, and Operation Glowing Symphony. Irresponsible operations would include developing and deploying the WannaCry virus. As a result, irresponsible operations should be condemned and seen as breaching international law and the Geneva conventions. This should still apply even if the attributed nation state, and/or sponsored groups, deny being behind the attack. The ethical question any stakeholder of responsible offensive operations has to take into consideration is how to prevent irresponsible operations. Further studies in offensive operations to prevent irresponsible operations are needed because not all nation states or sponsored groups adhere to international law and the laws of armed conflict. These studies should also consider how they can improve deterrence. Offensive operations will continue to play an important role in nation state to nation state competition, both in cyberspace and in space.

References


MITRE. (N.d.) Collection. Retrieved from https://attack.mitre.org/tactics/TA0009/


MITRE. (N.d.) Social Engineering. Retrieved from https://attack.mitre.org/techniques/T1279/


OWASP. (2010). Application Denial of Service. Retrieved from
Retrieved from https://www.justsecurity.org/64669/top-expert-backgrounder-on-aborted-u-s-strike-and-cyber-
operation-against-iran-and-international-law/.
Tran, Khai. (N.d.). Basic Web Exploitation Techniques. Retrieved from
https://www.academia.edu/1748466/Basic_Web_Exploitation_Techniques.