Anticipatory Ethics for Vulnerability Disclosure

Gazmend Huskaj[1, 2] and Richard L. Wilson[3, 4]
[1]Swedish Defence University, Stockholm, Sweden
[2]University of Skövde, Sweden
[3]Towson University, USA
[4]Senior Research Scholar, Hoffberger Center for Professional Ethics, University of Baltimore
gazmend.huskaj@fhs.se
wilson@towson.edu
DOI: 10.34190/ICCWS.20.053

Abstract: This article presents the ethical dilemma related to under what circumstances vulnerabilities should be disclosed. Vulnerabilities exist in hardware and software, and can be as a consequence of programming errors or design flaws. Threat actors can exploit these vulnerabilities to gain otherwise unintended access to information systems, resources and/or stored information. In other words, they can be used to impact the confidentiality, integrity and availability of information in information systems. As a result, various types of vulnerabilities are highly sought after since they enable this type of access. The most highly sought are so-called "zero-day"-vulnerabilities. These are vulnerabilities that exist but are unknown, and when exploited, enable one way of entry into a system that is not thought possible. This is also why zero-day vulnerabilities are very popular among criminal organizations, states and state-sponsored advanced persistent threats. The other side of the coin is when a state identifies a zero-day, and ends up in the ethical dilemma of whether to release the news and inform the vendor to patch it, i.e. close the vulnerability, or to use it for offensive or intelligence purposes. This article employs these distinctions to apply anticipatory ethics in the Stuxnet-case. Stuxnet was a computer software that was allegedly developed by the U.S. together with Israel to disrupt Iran's development of uranium for their nuclear program. More exactly, it was developed to disable the uranium centrifuges used to enrich uranium. To achieve this, Stuxnet exploited four zero-day vulnerabilities and, according to some experts, managed to delay Iran's nuclear program by one to two-years, forcing them to the negotiation table. Using vulnerabilities like zero-days presents opportunities but also risks. The results of the application of anticipatory ethics to the Stuxnet case are then compared with the "Osirak"-case and the "al-Kibar"-case. Osirak was the nuclear reactor in Iraq and was bombed in 1981; al-Kibar was the nuclear reactor being built up in Syria, also bombed in 2007.

Keywords: Vulnerabilities, Zero-Days, Information Systems, Ethical Dilemma, Stuxnet, Iran Nuclear Program, Anticipatory Ethics

1. Introduction

This article presents the ethical dilemmas related to computer vulnerabilities that, under certain circumstances should be disclosed. Vulnerabilities exist in hardware and software, and can be seen as a consequence of programming errors or design flaws. One 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 a vulnerability 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.' Threat actors can exploit these vulnerabilities for offensive cyberspace operations to gain otherwise unintended access to information systems, resources and/or stored information (Huskaj, 2019). In other words, they can be used to impact the confidentiality, integrity and availability of information in information systems. The reasons for exploiting these vulnerabilities can be varied; to steal intellectual property, to plant 'logic-bombs' in critical infrastructure, or for intelligence purposes. The most highly sought-after vulnerabilities are so-called "zero-day"-vulnerabilities. These are vulnerabilities that exist but are unknown, and when exploited, they enable one way of entry into a system that is otherwise not thought possible. This is also why zero-day vulnerabilities are very popular among criminal organizations, states and state-sponsored advanced persistent threats.

2. The Cases

Stuxnet was software that altered the rotation speed of uranium enrichment centrifuges. The information relevant to this analysis is the revelation of Stuxnet's existence and the result of many security researchers' work. Stuxnet altered the rotation speed of uranium enrichment centrifuges which resulted in Iran's failure to enrich uranium. The intent was to use that uranium to develop nuclear weapons. The Iranian government however stated that the purpose was to use it for nuclear power plants. However, the U.S., Israel and several

other countries were not convinced. Allegedly, Israel pushed to intervene and had meetings with the US government, who decided against using force. The preferred course of action was to use cyber capabilities to affect the program. Information revealed that the information systems managing the centrifuges were air gapped, i.e. not connected to the Internet. Security also showed they used the Microsoft Windows operating system (OS) and Simatic WinCC SCADA systems (Naraine, 2010).

A testbed was created using the same version of the OS and the SCADA systems. The development of the software was spread around the research labs of the U.S. government for operation security (OPSEC) reasons. The first step was to solve the problem of the air-gapped infrastructure. The second was to execute the software in the air gapped infrastructure. The third was to change the rotation frequency of the centrifuges. The fourth was that all of this would have to be done covertly.

Solving the air-gap problem involved getting a human to do the job. The most convenient way turned out to use a USB-memory stick. The requirement to execute the software on the target system was for it to execute automatically, without human action. The first attack in 2007 involved to overpressure centrifuges while the second attack in 2010 involved changing the rotation frequency (Langner, 2013). Changing the rotation frequency of the centrifuges required specific knowledge of the SCADA systems controlling the centrifuges. Doing this covertly meant having a high classification of the operation in general.

Naraine (2010a) stated that “The attackers behind the recent Stuxnet worm attack used four different zero-day security vulnerabilities to burrow into -- and spread around -- Microsoft's Windows operating system.” The four zero days exploited a .lnk file vulnerability, “a remote code execution vulnerability as well as two local privilege escalation vulnerabilities” (Murchu, 2010).

The .lnk file vulnerability allowed “local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer” (NVD, 2010a). The issue at hand was improper input validation. Improper input validation is “when software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.” (MITRE, 2019).

The remote code execution vulnerability “does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory, and consequently execute arbitrary code” (NVD, 2010b). The same issue that was identified above was here: improper input validation.

The two local privilege escalation exploits targeted vulnerabilities in Keyboard layout file and Task Scheduler (Naraine, 2010b). The first one loaded an index without verification, allowing the “the malware to force the system’s kernel to execute code controlled from the user area” (xmco, 2011, p.16). The second one modified the task file to create a CRC32 collision, allowing an attacker to “execute arbitrary commands with SYSTEM privileges” (webDEViL, 2010).

The Osirak/Osiraq-case, or “Operation Opera”, was an Israeli air operation that destroyed Saddam Hussein’s nuclear plutonium reactor in 1981. In 1977, Israel discovered that Iraq was developing a nuclear reactor. At their disposal, the Israeli had F-4 Phantoms and Skyhawks which “were not capable of flying the over 1,000 miles into enemy territory and returning safely” (TOI, 2019). However, during the 1978-1979 Islamic Revolution in Iran, 75 U.S. F16s intended for the country were cancelled and redirected to Israel (TOI, 2019). Accounts of the type of aircraft used in the operation differed. Shipler (1981) noted that “American military analysts said that the bombing was apparently done by American-made F-4 Phantoms escorted by F-15’s.” Evans (2017) on the other hand notes “fourteen American-built F-16 fighter aircraft had taken off from an Israeli airstrip in the Negev.” However, according to the IAF commander in 1981, Maj.Gen. David Ivry, “eight aircraft instead of the originally planned four” were used (TOI, 2019). These were F16s.

Ten Iraqi soldiers and one French technician were killed in the attack (BBC, 2006). The Italian Government reported that “none of the 20 Italian technicians at the project had been injured” (Lewis, 1981). The consequences of the attack were condemnations from the British Foreign Office, the Secretary General of the United Nations, and the Soviet Union (Lewis, 1981), and according to a U.S. Intelligence assessment, the “attack has hurt US interests” (Evans, 2017).

The al-Kibar-case, or "Operation Outside the Box", was an Israeli air operation destroying Bashar al-Assad's suspected nuclear reactor in 2007. In 2004, Israeli intelligence believed North Korea was helping Syria to build a nuclear reactor (BBC, 2018). In 2006, Israel had additional information that confirmed the details of the situation. At 22:30 on 5 September 2007, four F15 and four F16 aircraft flew to Deir al-Zour and bombed the nuclear reactor (BBC, 2018). Israel "verified that the reactor was destroyed 'beyond any chance of rehabilitation'" (Opall-Rome, 2018) on 6 September 2007 at 02:30. There is no information about the death toll during the attack.

3. Vulnerabilities and vulnerability disclosure

This section describes vulnerabilities and the vulnerability disclosure process (VEP). "A vulnerability is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm" (Pfleeger & Pfleeger, 2012, p.10). Vulnerabilities enable access to information systems. In the Stuxnet case, four zero-day vulnerabilities were used, and a fifth vulnerability was already known. Table 1 shows the zero-days and the non-zero-day vulnerability.

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

Table 1: Zero-days and non-zero-day vulnerabilities

		Impact						
Name	Vulnerability Type	Confidentiality	Integrity	Availability	Access Complexity	Authentication	Gained Access	CVE
.lnk	Execute Code	Complete	Complete	Complete	Medium	Not required	None	CVE-2010-2568
Print Spooler Service Impersonation	Execute Code	Complete	Complete	Complete	Medium	Not required	None	CVE-2010-2729
Win32k Keyboard Layout	Gain Privileges	Complete	Complete	Complete	Low	Not required	None	CVE-2010-2743
Task Scheduler	Gain Privileges	Complete	Complete	Complete	Low	Not required	None	CVE-2010-3338
Server Service	Execute Code Overflow	Complete	Complete	Complete	Low	Not required	Admin	CVE-2008-4250

The problem for vendors is whether customers should be notified of the existence of these vulnerabilities. The purpose of the VEP is "to balance equities and make determinations regarding disclosure or restriction when the USG obtains knowledge of newly discovered and not publicly known vulnerabilities in information systems and technologies" (The White House, 2017, p.1). Managing vulnerabilities responsibly is important because of the "significant economic, privacy and national security implications [they can have] when exploited" (The White House, 2017, p.2). The process is not led by a single agency, rather, it is "coordinated by the National Security Council (NSC) staff so that multiple agency viewpoints can be considered, informed by the full input and consideration of the interagency experts" (The White House, 2017, p.2). The process has a threshold for vulnerabilities whether they are worthy to be considered for the VEP or not. The threshold is that the vulnerability "must be both newly discovered and not publicly known" (The White House, 2017, p.5). If the vulnerability meets this requirement it is then submitted to the VEP Executive Secretariat. The submission "will include, at a minimum, information describing the vulnerability, identification of the vulnerable products or systems, and a recommendation on dissemination of the vulnerability information" (The White House, 2017, p.7). Next, equity and discussions take place to disseminate or restrict information about the vulnerability. If consensus is reached, the Equities Review Board (ERB) ratifies a recommendation for further actions such as "sharing, restricting or reassessing" (The White House, 2017, p.7).

4. Understanding Ethics

This section describes the ethical issues with the disclosure of zero-day vulnerabilities. Zero-day vulnerabilities present the possibility of developing exploits which can be used to generate deny, degrade and destroy effects, but also deceive and manipulate effects. 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 particular variations are presented here. The first one is the ethical issues related to zero-day vulnerabilities are based upon the idea that those who discover them have taken actions to discover them, and these actions are an extension of what a person intends. The second is that the actions to discover zero-day vulnerabilities are capable of being evaluated based upon the intentions and actions of the people engaged in those activities, as well as the outcomes of their actions. Likewise, the action to disclose or not is capable of being evaluated based on those responsible for making that decision. Applying Furrow's (2005) distinctions to zero-day vulnerabilities leads us to three possible levels of ethical evaluation. First, the actions of a person performing actions to discover zero-day vulnerabilities, and the action/decision to disclose it or not. Second, the intentions of a person's actions to discover zero-day vulnerabilities. Third, the nature of the act, or the consequences of the actions intended by the person(s) discovering zero-lady vulnerabilities and their action/decision to disclose them or not.

The actions of agents discovering zero-day vulnerabilities are subject to ethical evaluation based on the actions of the person(s) decision to disclose or not, the intentions or motives of that person, and the consequences produced by disclosing or not disclosing zero-day vulnerabilities. Using Furrow's distinctions (2005), it is ultimately the person or persons who are deciding whether to disclose or not zero-day vulnerabilities that are subject to moral evaluation. Identifying the ethical issues with zero-day vulnerabilities, requires asking four questions: 1) what actions are performed when disclosing or not a zero-day vulnerability; 2) what is the character of the person(s) taking those decisions; 3) what are the intentions of those deciding whether disclosure should or should not occur; and 4) what are the consequences of disclosing or not disclosing zero-day vulnerabilities.

The ethical issues with zero-day vulnerabilities are the result of how they are exploited and the potential consequences if they are not disclosed. The purpose of withholding knowledge of a zero-day vulnerability is to achieve tactical, operational or strategic goals by that person or persons. In this case there is the controller of a zero-day vulnerability, and those affected by the exploit of zero-day vulnerabilities. The intention of the person or persons engaged in exploiting zero-day vulnerabilities involves instrumental reasoning and establishing a purpose for exploiting zero-day vulnerabilities, as well as a goal (such as degrading a nuclear weapon program). Next is the adversary's nuclear weapon program which poses an existential threat affected by the purpose of zero-day vulnerabilities, which involves the technical issue of affecting the information systems responsible for uranium enrichment centrifuges. The interaction between the technical use of a software exploiting a zero-day vulnerability by the person or persons to affect a uranium enrichment centrifuges, and the technical effect of the exploit as it affects information systems and industrial and control systems, is where ethical issues with disclosing or not zero-day vulnerabilities arise. A preliminary ethical analysis can be developed by applying standard ethical principles. With appropriate space and time these standard ethical principles can be applied to how the intentions of the person(s) deciding whether to disclose or not zero-day vulnerabilities, with the actions of disclosing or not disclosing zero-day vulnerabilities, and with outcomes of disclosing or not disclosing zero-day vulnerabilities, are ethically responsible or not.

5. Stakeholders

This section describes the stakeholders in the three cases under discussion. In the Stuxnet-case, the stakeholders were Israel, Iran, the U.S., and the neighboring countries. In the Osirak(q) case, the stakeholders were Israel, Iraq, France, Italy and the U.S., while in the al-Kibar case, the stakeholders were Israel, Syria, and the neighboring countries. Table 2 depicts the stakeholders.

Table 2: The various stakeholders in the three cases

Stakeholders	Osirak(q)	al-Kibar	Stuxnet
France	x		
Iran			x
Iraq	x		
Israel	x	x	x
Italy	x		
Syria		x	

Stakeholders	Osirak(q)	al-Kibar	Stuxnet
U.S.	x		x
Neighboring Countries		x	x

The Iranian government was and is continuing to pursue the development of nuclear weapons. The nuclear facility in Natanz shows their intent to enrich uranium, and as long as the Iranians pursue this course of action, they will be perceived as an existential threat to Israel. In the al-Kibar-case, when al-Assad was working to repair relations with the West, Iran sent a government representative calling "Assad's plan 'unacceptable' and threatened that it would spell the end of the two countries' strategic alliance and a sharp decline in relations" (Follath & Stark, 2009).

From Israel's perspective, Countries "hostile to Israel and that call for its destruction must not be allowed to develop a nuclear military capability that could be used against Israel" (Yadlin, 2018). This is also known as "the Begin Doctrine." Based on this doctrine, Israel conducted air strikes in Iraq and Syria. A different course of action was chosen against Iran: using cyber-tools to affect the program.

Iraq was working to develop nuclear weapons in the 1970s (NTI, 2019). It was cooperating with France and Italy to receive the necessary equipment for it.

Syria was developing a nuclear reactor covertly with the help of North Korea. The development of the reactor was done without the knowledge of Russia. After the nuclear program was destroyed, al-Assad was looking to repair relations with the West.

The US condemned the attack on Osirak(q). Jeane J. Kirkpatrick, an American delegate to the United Nations, said that the US was "shocked by the Israeli air strike, which exacerbated deeper antagonisms in the region" (Nossiter, 1981). Having said that, Kirkpatrick noted after a UN resolution that "nothing in the resolution will affect my Government's commitment to Israel's security" (Nossiter, 1981). Now to the details of the "al-Kibar"-case. The US was informed that al-Bashar was working with North Korea to develop a nuclear reactor in northern Syria. However, the CIA wanted to make sure that the threat was real, a harsh lesson was learned that Saddam Hussein had weapons of mass destruction (Follath & Stark, 2009). In the "Stuxnet"-case, the US was unwilling to help Israel with a request on "bunker-busting bombs" (Sanger, 2009). However, they had developed a cover program since 2008 to "penetrate Iran's nuclear supply chain abroad, along with new efforts, some of them experimental, to undermine electrical systems, computer systems and other networks on which Iran relies. It is aimed at delaying the day that Iran can produce the weapons-grade fuel and designs it needs to produce a workable nuclear weapon" (Sanger, 2009).

France condemned the attack. The French Foreign Ministry said the "main reactor, which uses highly enriched uranium fuel suitable for atomic weapons, was 'seriously damaged'" (Lewis, 1981). Of the 150 French citizens working at the site, one technician was killed.

Italy "said that none of the 20 Italian technicians at the project had been injured" (Lewis, 1981). They were working on the site to manage radioactive materials.

Neighboring countries posed a threat to the operation. The designers of the air strike in Osirak noted this threat and plotted a dogleg course "to best avoid detection by Jordanian radar to the north and the Saudi E-3 Airborne Warning and Control System operating to the south" (Correll, 2012, p. 61).

6. Technical / professional problems

This section depicts the technical / professional problems with the three cases. These problems are clustered in centrifuges, hardware and software; fighter jet distance, and adversary technical threats.

Centrifuges, Hardware and Software. The technical problem was to identify the type of centrifuge, the hardware, the software and the related vulnerabilities to exploit. Then, a testbed had to be developed with the centrifuges, and related hardware and software. In addition, the software that was going to exploit the vulnerabilities and degrade the uranium enrichment process had to be developed and tested.

Fighter jet distance. The al-Kibar-case required the F-4 Phantoms and Skyhawks to fly over 1,000 miles. These fighter aircraft did not have the required capability. This technical problem was solved by acquiring the modern F16s. The professional problem to pilot the new F16s was solved by having the pilots train in the US.

Adversary technical threats. The technical threats consisted of radar systems, missile systems and users. The threats stemming from radar and missile systems were managed as follows: avoid detection by plotting a "dogleg course" (Correll, 2012, p. 61); using electronic warfare and "military computer hacking and electronic intelligence methods [and disabling] two radar systems" (Evans, 2017). The users in the Stuxnet-case were tricked by showing a picture of the sensors as if nothing was wrong with the centrifuges.

7. Ethical problems

The ethical issues with these technologies is how they can be used by actors in each case to conduct air strikes, electronic warfare and hacking, and exploiting zero-day vulnerabilities. These technologies are used by professional trained pilots, sabotage units, electronic warfare (EW) units, and cyberspace operators. There is the controller of each capability, i.e. pilots, sabotage personnel, EW-personnel, and cyberspace operators, and the targets affected by the activities of pilots, sabotage personnel, EW-personnel, and cyberspace operators. The intentions of the pilots, sabotage personnel, EW-personnel, and cyberspace operators involves reasoning and establishing a purpose for the use pilots, sabotage personnel, EW-personnel, and cyberspace operators, as well as a goal. The targets affected by the purpose of pilots, sabotage personnel, EW-personnel, and cyberspace operators, involves the technical issues of bombs, ground attacks, and non-kinetic warfare. The interaction between the technical use of pilots, sabotage units, EW, and cyberspace operations to destroy or degrade nuclear programs and the technical effect of pilots, sabotage units, EW, and cyberspace operations as it affects nuclear programs and the people involved, are where ethical issues arise.

8. The social consequences of vulnerabilities

Vulnerabilities and zero-days in information systems can have negative effects on society and on global relations. Information systems that can be exploited can be a part of a banking system, financial system, or critical infrastructure. Not disclosing identified vulnerabilities and zero-days in these systems pose the risk of adversaries identifying these vulnerabilities and exploiting them for their own purposes. Affecting a banking system could lead to the inability of withdrawing funds; attacking a financial system could make it difficult or impossible for companies to do business; attacking critical infrastructure which could lead to society being without power.

9. Technical Conclusions

Air strikes and cyberspace operations were used to degrade and destroy nation states' nuclear programs posing an existential threat to Israel. The air strikes in 1981 and 2007 received a great deal of international criticism and condemnation. Not only did the air strikes breach international law by flying into another country's territory, but they also led to the death of people and destruction of facilities. The alleged U.S. and Israeli cyberspace operation never received the same media-attention as the air strike-operations. It also never received the attention of the users and decision-makers in Iran working in their nuclear program. The ethical issue with neutralizing threats through air strikes and the likelihood of casualties, shows the level of risk that was involved. This can be compared to the ethical issue of not disclosing vulnerabilities and using exploits to degrade a nuclear program, which leads to a significant lower level of risk and less possibility of receiving international condemnation and casualties. Another major element here is the difficulty of attribution for attacks such as the Stuxnet attack.

10. Policy Related Ethical Analysis

The continual advances in technology result in society's greater dependency on this technology. At the same time, it is known that there are underlying hardware and software contains vulnerabilities. It is therefore important to identify possible problems and attempt to anticipate ethical problems. Identifying possible problems and anticipating ethical problems can be used as the basis for policy development. Therefore, the vulnerability equity process was developed to assist decision-making whether to disclose or restrict the knowledge about zero-day vulnerabilities in hardware and software. Hardware and software consist of computer artifacts. A group of scholars met to discuss "ethical guidance for the research and application of pervasive and autonomous information technology" (Miller, 2011, p. 57). The resulting document was dubbed to "Principles Governing Moral Responsibility for Computing Artifacts" (Miller, 2011, p. 57) and consists of five

rules about moral responsibility for computing artifacts. These rules will be used to develop policy recommendations. Moral responsibility is "that people are answerable for their behavior when they produce or use computing artifacts" (Miller, 2011, p. 57). 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 could be extended to those discovering zero-days. Discovering zero-days involves actions performed on software and hardware to put the hardware and software in a state the developers never intended the software and hardware to be in. For example, the developer(s) of fingerd and sendmail in the 1988-Morris-case never intended the software to receive more than 512 bytes of instructions. However, Morris took actions and found that by sending a 536-byte request he could execute code on the target system. The application of this rule for policy would be that those discovering zero-days should not disclose them in cases of existential threats where actions to manage the threats could lead to international condemnation.

The second rule of the five states, "The shared responsibility of computing artifacts 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 artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person." This second rule could be applied to the discovery of zero-day vulnerabilities would state that those discovering zero-days are responsible for how that zero-day is exploited. Applying this to the al-Kibar and Osiraq(k)-cases means that the pilots, sabotage units and EW-operators are responsible for how they exploited their capabilities.

The fourth rule of the five rules is, "People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded." One application of this rule would be that those discovering a zero-day and who know it will be exploited to manage an existential threat should exploit it responsibly and should not disclose it.

11. Anticipatory Ethical Recommendations/Policy

Anticipatory ethics can be used to develop policy recommendations when it is used conjunction with the conclusions of the preceding application of the five rules for computing artifacts. It is anticipated that existential threats from an adversary will always be met with a combination of kinetic and non-kinetic response. The response is the result of the adversary's intent to gain a capability once it is complete and if it is used, poses an existential threat. The Stuxnet-case shows how zero-day vulnerabilities in hardware and software were exploited to degrade the nuclear program of Iran. It did so "under the radar", and it was not until the software came out of its target that it was revealed to the world. Even then it never received any international condemnation because it was difficult to attribute it. This would have never been possible if the exploited zero-day vulnerabilities had been disclosed. If these zero-day vulnerabilities had been disclosed, the first option, to use "bunker-bombs" may have been applied. The results would have then been likely to have reflected the results of the al-Kibar and Osirak(q)-cases: which included high levels of risk to pilots, sabotage units, EW-personnel, personnel working at the nuclear program-facilities, while also risking armed conflict with neighboring countries. The exploitation of zero-day vulnerabilities in the Stuxnet-case removed all those risks. The lessons learned from the Stuxnet case give a good indication of what needs to be anticipated about future cases involving vulnerability disclosure.

References

BBC. (2006). Factfile: How Osirak was bombed. Retrieved from http://news.bbc.co.uk/2/hi/middle_east/5020778.stm.

BBC. (2018). Israel admits striking suspected Syrian nuclear reactor in 2007. Retrieved from https://www.bbc.com/news/world-middle-east-43481803.

Correll, John. T. (2012). Air Strike at Osirak. http://www.airforcemag.com/MagazineArchive/Documents/2012/April%202012/0412osirak.pdf

Evans, A. (2017). A Lesson from the 1981 Raid on Osirak. Retrieved from https://www.wilsoncenter.org/blog-post/lesson-the-1981-raid-osirak.

Evans, Mike. (2017). An Attack on A Syrian Reactor: Ten years after a tell-all in the New Yorker, remembering the Israeli operation to destroy Syria's reactor. Retrieved from https://www.jpost.com/Opinion/An-attack-on-a-Syrian-reactor-504735.

Follath, Eric., Stark, Holger. (2009). The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor. Retrieved from https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-4.html.

Herzog, M. (2016). Iran Still Looms Large in Israel's Threat Perception. Retrieved from https://www.washingtoninstitute.org/policy-analysis/view/iran-still-looms-large-in-israels-threat-perception.

Huskaj, G. (2019). The Current State of Research in Offensive Cyberspace Operations. Proceedings of the 18th European Conference on Cyber Warfare and Security ed. By Tiago Cruz and Paulo Simoes, Academic Conferences and Publishing Limited. Reading UK.

Langner, R. (2013). To kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Retrieved from https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Lewis, P. (1981). France Condemns Attack and Rejects Israeli Account. Retrieved from https://www.nytimes.com/1981/06/09/world/france-condemns-attack-and-rejects-israeli-account.html

Lewis, Paul. (1981). France Condemns Attack and Rejects Israeli Account. Retrieved from https://www.nytimes.com/1981/06/09/world/france-condemns-attack-and-rejects-israeli-account.html.

Microsoft. (2008). Microsoft Security Bulletin MS08-067 - Critical. Retrieved from https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067.

Miller, K. W. (2011). Moral responsibility for computing artifacts: "The rules." IT Professional, 13(3), 57–59. https://doi.org/10.1109/MITP.2011.46

MITRE. (2019). CWE-20: Improper Input Validation. Retrieved from http://cwe.mitre.org/data/definitions/20.html.

Murchu, L.O. (2010). Stuxnet Using Three Additional Zero-Day Vulnerabilities. Retrieved from https://www.symantec.com/connect/blogs/w32stuxnet-installation-details.

Naraine, R. (2010a). Stuxnet attackers used 4 Windows zero-day exploits. Retrieved from https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/.

Naraine, R. (2010b). Attack code published for unpatched Stuxnet vulnerability. Retrieved from https://www.zdnet.com/article/attack-code-published-for-unpatched-stuxnet-vulnerability/.

Nossiter, Bernard. D., (1981). Israelis Condemned by Security Council for Attack on Iraq. Retrieved from https://www.nytimes.com/1981/06/20/world/israelis-condemned-by-security-council-for-attack-on-iraq.html.

NTI. (2019). Iraq. Retrieved from https://www.nti.org/learn/countries/iraq/.

NVD. (2010a). CVE-2010-2568 Detail. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2010-2568.

NVD. (2010b). CVE-2010-2729 Detail. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2010-2729.

Opall-Rome, B. (2018). Declassified: How an Israeli operation derailed Syria's nuclear weapons drive. Retrieved from https://www.defensenews.com/global/mideast-africa/2018/03/20/just-declassified-how-an-israeli-operation-derailed-syrias-nuclear-weapons-drive/.

Pfleeger, C. P., & Pfleeger, S. L. (2012). Analyzing Computer Security (1st ed.). Prentice Hall.

Sanger, David. E., (2009). U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site. Retrieved from https://www.nytimes.com/2009/01/11/washington/11iran.html.

Shipler, D.K. (1981). Israeli Jets Destroy Iraqi Atomic Reactor; Attack Condemned by U.S. and Arab Nations. Retrieved from https://www.nytimes.com/1981/06/09/world/israeli-jets-destroy-iraqi-atomic-reactor-attack-condemned-us-arab-nations.html.

The White House. (2017). Vulnerabilities Equities Policy and Process for the United States Government. Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

TOI. (2019). 38 years later, pilots recall how Iran inadvertently enabled Osiraq reactor raid. Retrieved from https://www.timesofisrael.com/38-years-later-pilots-recall-how-iran-inadvertently-enabled-osiraq-reactor-raid/.

WebDEViL. (2010). Microsoft Windows - Task Scheduler Privilege Escalation. Retrieved from https://www.exploit-db.com/exploits/15589.

Wilson, Richard L., Cambridge Analytica, Facebook, and Influence Operations: A Case Study and Anticipatory Ethical Analysis. Proceedings of the 18th European Conference on Cyber Warfare and Security ed. By Tiago Cruz and Paulo Simoes, Academic Conferences and Publishing Limited. Reading UK, 2019

Wilson, Richard L., Cyber Warfare, Terrorist Narratives and Counter Terrorist Narratives: An Anticipatory Ethical Analysis. Proceedings of the 18th European Conference on Cyber Warfare and Security ed. By Tiago Cruz and Paulo Simoes, Academic Conferences and Publishing Limited. Reading UK, 2019

Xmco. (2011). ACTUSÉCU 27. Retrieved from https://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET_EN.pdf.

Yadlin, A. (2018). The Begin Doctrine: The Lessons of Osirak and Dear ez-Zor. Retrieved from https://www.inss.org.il/publication/the-begin-doctrine-the-lessons-of-osirak-and-deir-ez-zor/.