A Realistic Analysis of the Stuxnet Cyber-attack

By: Ahmad Mohee

MA Arabic Studies – Political Sciences

Cairo on 1st March 2022

Abstract

The Iranian-Israeli conflict has taken an accelerating dangerous turn. The pace and momentum of the reciprocal cyber-attacks have accelerated from the two sides, since the Stuxnet attack was first revealed in 2010. Analysts have come to use the term “cyber war” without hesitation to describe the reciprocal cyber-attacks between Iran and Israel.

This paper presented a realistic analysis of Stuxnet cyber-attack, aiming to uncover the complexities associated with the launch decision-making process. It managed to answer the question: Why were Stuxnet cyber-attack adopted, as a strategic choice for managing the conflict instead of traditional choices? It also gave an understanding for the security challenges and the strategic implications that cyber-attack had to pose.

Finally, it reached a number of conclusions to the effect that: Realism, as a theory mostly concerned with issues of national security and power, can be a very suitable theoretical framework for analyzing and understanding cyber-attacks. The analysis confirmed that realism is an appropriate framework for identifying important issues related to security in the cyberspace and can provide useful insights into some of the enduring characteristics of international relations in the cyberspace.

Keywords: Cyberwar, Cyber-attack, Stuxnet, Realism, International Relations, Iran, Israel

Introduction:

In May 2011, the Pentagon announced an official list of cyber weapon capabilities approved for use against adversaries. The list included a "toolkit" of methods to hack foreign networks, examine and test their functionality and operations, and the ability to leave "viruses" to facilitate future targeting[1].

Several months before that, in July 2010, the Iranian-Israeli conflict seemed to have taken a dangerous and accelerating turn, as the details of the cyber-attack on the Iranian Natanz nuclear facility were revealed using a virus or a "malicious computer worm" called Stuxnet[2].

The attack revealed the possibility of causing massive physical destruction in industrial facilities or vital infrastructure networks of any state without the need to mobilize armies or move fleets.

The pace and momentum of reciprocal cyber-attacks accelerated between the two sides since the Stuxnet attack was first revealed in 2010. Analysts have come to use the term "cyber war" without hesitation to describe the reciprocal cyber-attacks between Iran and Israel.

This was accompanied by a large cloud of controversy, mutual accusations, and theories that sought to probe the depths of the new term emerged in the skies of political circles: "cyber war".

This research paper aims to:

- Answer the question: Why were cyber-attacks adopted in the case of the Stuxnet, as a strategic option for conflict management instead of the traditional options?
- Apply the analysis of Realism to the case of Stuxnet, in order to understand the security challenges and the strategic effects it poses.
- Reach conclusions within the framework of Realism analysis.

[1] Nakashima, E. (2011). List of cyber-weapons Developed by Pentagon to Streamline Computer Warfare. The Washington Post. [online] 1 Jun. Available at: https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html [Accessed 28 Feb. 2022].

[2] Fruhlinger, J. (2017). What Is Stuxnet, Who Created It and How Does It work? [online] CSO Online. Available at: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [Accessed 28 Feb. 2022].

Stuxnet Capabilities

Once announced, specialists had been engaged in Stuxnet analysis for several months, to determine how it got into the control systems of the target industrial equipment, which were offline by nature, the type of systems, equipment, processes targeted, the entities that were attacked, and the functions the virus used to achieve the goals of the attack.

The requirements for analyzing this cyber-attack in terms of the tools and expertise used, the time required to reveal its capabilities and objectives, the estimation of the resulting damage levels, and the appropriate defense strategies and procedures, were completely different from the requirements for analyzing attacks in conventional wars.

The Stuxnet virus surreptitiously infiltrates and takes over industrial control systems with the aim of sabotaging normal industrial operations. The malicious computer worm is inserted via a "hole" in the industrial control system through a removable device such as a USB memory stick[3]. The virus uses default Siemens passwords to access Windows operating systems running WinCC and PC7 programs[4].

According to Ralph Langner, Stuxnet contained two different digital warheads, which were deployed together to present a "massive cyber strike against Iran's nuclear energy program." The first cyber warhead worked against Siemens S7-315 controllers, temporarily preventing legitimate software from taking control. The "Warhead" code handled up to 186 high-speed engines by rotating operating speeds between low and high values. The second cyber warhead, the Siemens 417 attack code, intercepted physical I/O and "provided forensic software running on the console with the normal input patterns pre-recorded by Stuxnet"[5].

Langer likens the process to a form of gimmick usually depicted in Hollywood movies; Surveillance during the robbery is replaced by pre-recorded security camera footage to fool the authorities into believing that nothing is unfamiliar[6].

If a nuclear centrifuge was indeed the target, the centrifuges needed to spin at a specific speed for long periods of time in order to extract the uranium. Stopping this process at high speeds could disrupt the sequestration of heavy isotopes in centrifuges. Tampering

[3] Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

[4] Eric Byres, P. (2011). Stuxnet Report: A System Attack. [online] ISSSource. Available at: https://isssource.com/stuxnet-report-a-system-attack/ [Accessed 28 Feb. 2022].

[5] Langner, R. (2010). The Big Picture. [online] Langner Blog. Available at: https://www.langner.com/2010/11/the-big-picture/ [Accessed 28 Feb. 2022].

[6] Langner, R. (2011). How to Hijack a Controller: Why Stuxnet Isn't Just about Siemens' PLCs. [online] Control Global. Available at: https://www.controlglobal.com/articles/2011/industrialcontrollers1101/ [Accessed 28 Feb. 2022].

with the motors in a gas centrifuge may lead to cracking and destruction of these components[7].

The target: Iran

Iran emerged as a potential target for the Stuxnet virus based on the geographical extent of the infection, which suggested that Iran was the epicenter of the attacks, and also on technical analyzes that revealed that Stuxnet could, at least in theory, “disable or destroy” Iran’s centrifuges[8].

Researchers have found out that the Stuxnet attack began in June 2009, and the time frame between compiling the source code and launching the infection was only about 12 hours, indicating that “the attackers had immediate access to the computer they used to spread the virus — either by working with an insider or inadvertently using a knowledgeable person to introduce the infection”[9].

The products of Siemens, the manufacturer of the target systems, were widely used in Iran's power and communications plants, and in Iran’s first nuclear power plant near Bushehr. It is possible that Stuxnet spread via contractors or over LANs to its expected target, the Natanz reactor[10].

Who Did It: Israel

Israel has been featured as the actor behind the Stuxnet attack in numerous media reports[11] [12] [13] [14] [15].

[7] Langner, R. (2013). To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve. The Langner Group.

[8] Broad, W.J. and Sanger, D.E. (2010). Worm Was Perfect for Sabotaging Centrifuges. The New York Times. [online] 19 Nov. Available at: https://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html [Accessed 28 Feb. 2022].

[9] Zetter, K. (2011). Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant. [online] Wired. Available at: https://www.wired.com/2011/02/stuxnet-five-main-target/ [Accessed 28 Feb. 2022].

[10] Nakashima, T.E. and E. (2010). Iran Struggling to Contain “foreign-made” “Stuxnet” Computer Virus. The Washington Post. [online] 28 Sep. Available at: https://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html [Accessed 28 Feb. 2022].

[11] Beaumont, P. (2010). Stuxnet Worm Heralds New Era of Global Cyberwar. [online] the Guardian. Available at: https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar [Accessed 28 Feb. 2022].

[12] Sanger, D.E. (2012). Obama Order Sped up Wave of Cyberattacks against Iran. The New York Times. [online] 1 Jun. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [Accessed 28 Feb. 2022].

[13] Halliday, J. (2010). Stuxnet Worm Is the “work of a National Government agency.” The Guardian. [online] 24 Sep. Available at: https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency [Accessed 28 Feb. 2022].

[14] Hounshell, B. (2010). 6 Mysteries about Stuxnet. [online] Foreign Policy. Available at: https://foreignpolicy.com/2010/09/27/6-mysteries-about-stuxnet/ [Accessed 28 Feb. 2022].

Although Israel hadn't released any official comment over the Stuxnet cyber-attack, in 2010, it created the 8200 or SIGINT intelligence unit to pursue both offensive and defensive duties of cyberwar. This confirmed that cyberwar was now one of the pillars of Israel's defense doctrine[16] [17].

Earlier in 2009, Scott Borg, an expert in the US-CCU, suggested that Israel might prefer a cyber-attack on Iran's nuclear facilities rather than a military strike, a year before Stuxnet was discovered[18]. In late 2010, Burg stated, "Israel certainly had the ability to create Stuxnet…a tool like Stuxnet was the obvious weapon of Israel"[19].

Who Did It: United States of America

There were also clear indications of US involvement and cooperation with Israel[20] . It was reported that United States - within the framework of one of its most secret programs, initiated by the Bush administration and accelerated by the Obama's - sought to destroy Iran's nuclear program by new methods such as hacking Iranian computer systems[21].

United States was advised by an influential German think tank to target Iran's nuclear capabilities through "covert sabotage". Volker Perthes, director of the German government-funded Institute for Security and International Affairs, told US officials in Berlin that covert operations would be "more effective than a military strike" in curbing Iran's nuclear ambitions[22].

[15] Markoff, J. (2010). Stuxnet Worm Is Remarkable for Its Lack of Subtlety. The New York Times. [online] 27 Sep. Available at: https://www.nytimes.com/2010/09/27/technology/27virus.html [Accessed 28 Feb. 2022].

[16] Williams, D. (2009). Spymaster Sees Israel as World Cyberwar Leader. Reuters. [online] 15 Dec. Available at: https://www.reuters.com/article/idUSTRE5BE30920091215 [Accessed 28 Feb. 2022].

[17] Williams, D. (2010). EXCLUSIVE - Cyber Takes Centre Stage in Israel's War Strategy. Reuters. [online] 28 Sep. Available at: https://www.reuters.com/article/idINIndia-51792020100928 [Accessed 28 Feb. 2022].

[18] Williams, D. (2009). ANALYSIS-Wary of Naked force, Israelis Eye Cyberwar on Iran. Reuters. [online] 7 Jul. Available at: https://www.reuters.com/article/idUSLV83872 [Accessed 28 Feb. 2022].

[19] The Economist (2010). A Worm in the Centrifuge. [online] The Economist. Available at: https://www.economist.com/international/2010/09/30/a-worm-in-the-centrifuge [Accessed 28 Feb. 2022].

[20] Reals, T. (2010). Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes? [online] cbsnews.com. Available at: https://www.cbsnews.com/news/stuxnet-worm-a-us-cyber-attack-on-iran-nukes/ [Accessed 28 Feb. 2022].

[21] Kelley, M.B. (2012). Obama Administration Admits Cyberattacks against Iran Are Part of Joint US-Israeli Offensive. [online] Business Insider. Available at: https://www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2012-6 [Accessed 28 Feb. 2022].

[22] Halliday, J. (2011). WikiLeaks: US Advised to Sabotage Iran Nuclear Sites by German Thinktank. [online] The Guardian. Available at: https://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear [Accessed 28 Feb. 2022].

In a New York Times article published in January 2009, an unspecified program was credited with preventing an Israeli military attack on Iran, as some efforts focused on ways to destabilize the centrifuges[23].

Why Was A Cyber-attack Adopted As A Strategic Option To Manage The Conflict Instead Of Traditional Options?

The US and Israeli governments intended to use Stuxnet as a tool to impede, or at least delay, the Iranian nuclear program. The Bush and Obama administrations believed that if Iran was on the verge of developing nuclear weapons, Israel would launch air strikes against Iran's nuclear facilities in a move that could have triggered a regional war.

In early 2008, the Israeli government submitted a "secret" request to the Bush administration to provide it with bunker-busting bombs capable of destroying underground facilities; and refueling equipment to allow it to fly to Iran and back to Israel, with permission to fly over Iraqi airspace. However, the Bush administration "ignored" Israeli demands for bombs and refueling equipment and refused to use Iraqi airspace, over fears that doing so would cause a "political uproar" in Iraq that might lead to "the expulsion of American forces"[24].

The Bush administration decided to pursue a new covert effort as a result of the failure of sanctions to rein in Iran's uranium enrichment, and in light of the fact that options for military strikes seemed "unacceptable". The Bush administration turned to the CIA to help slow progress at Natanz and other "known and suspected nuclear facilities"[25].

A dramatic meeting took place in the White House Situation Room late in the Bush presidency, in which parts of a previously destroyed centrifuge were shown in an experiment on the table. At that time, United States gave the green light to the Operation Olympic Games, which included the Stuxnet cyber-attack[26].

Operation Olympic Games was an extensive covert program to delay Iran's ability to produce nuclear weapons broadly targeting "the entire industrial infrastructure that supports Iran's nuclear program" including efforts to "destabilize" centrifuges. The program also included "renewed US efforts to penetrate Iran's nuclear supply chain abroad, along with new, some experimental efforts to undermine the electrical systems, computer systems, and other networks that Iran relies on"[27].

[23] Sanger, D.E. (2009). U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site (Published 2009). The New York Times. [online] 10 Jan. Available at: https://www.nytimes.com/2009/01/11/washington/11iran.html [Accessed 28 Feb. 2022].

[24] Sanger, D.E. (2009). op. cit.

[25] Sanger, D.E. (2009). op. cit.

[26] Fruhlinger, J. (2017).op. cit.

[27] Sanger, D.E. (2009). op. cit.

Prior to leaving office in 2009, the Bush administration allocated $300 million to such secret joint projects with Israel against Iran[28]. The covert program appears to have been "accelerated" under the Obama administration, although what that entails has been shrouded in secrecy[29].

Realistic Analysis of the Stuxnet Cyber-attack

Realism has always been a dominant paradigm in the field of international relations. The field of cyber security shows a correlation with realist-influenced perspectives with a focus on security and competition, power distribution, the advantage of attack over defense, and the benefits of deterrence strategies. Although there is no theory of cyber power in realist literature, realism provides a framework for understanding the distribution of power among actors and how this relates to conflict[30].

According to Reardon and Choucri: "Realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilizing or destabilizing, whether cyber technologies will be a new source of conflict or of peace, and whether states will engage in cyber arms racing."[31].

Conflict Management Options and The Realism of USA

The repercussions that led to the development and launch of Stuxnet within the "Operation Olympic Games" refer to a realistic strategy on the American side for the options of conflict with Iran. A cyber-attack was not Israel's first choice in dealing with the threat of the Iranian nuclear program. Despite the strong alliance between United States and Israel, and the mutual security dependence between them, especially with regard to their interests in the Middle East, United States, within the framework of realistic decision-making guidance, saw that Israel's option to launch a conventional military strike on the Iranian nuclear program could be of a huge cost for both US and Israel.

And because the threat posed by the Iranian nuclear program was similar to both American and Israeli national security, undermining Iran's nuclear capabilities was a common strategic goal for the two states. However, United States sought with realism

[28] MacAskill, E. (2011). Stuxnet Cyberworm Heads off US Strike on Iran. [online] The Guardian. Available at: https://www.theguardian.com/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran [Accessed 28 Feb. 2022].

[29] Sanger, D.E. (2010). Iran Fights Malware Attacking Computers. The New York Times. [online] 25 Sep. Available at: https://www.nytimes.com/2010/09/26/world/middleeast/26iran.html [Accessed 28 Feb. 2022].

[30] Craig, A. (2013). Realism and Cyber Conflict: Security in the Digital Age. [online] E-International Relations. Available at: https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ [Accessed 1 Mar. 2022].

[31] Reardon, R., & Choucri, N. (2012, April). The role of cyberspace in international relations: A view of the literature. In ISA Annual Convention, San Diego, CA (Vol. 1).

and rationality to achieve its goals and self-interest to assert power and security in the region by offering the most realistic, least costly strategic option for its national security and the security of its ally, Israel.

The foregoing analysis could also be a reason why cyber warfare can sometimes not be fully adopted as a strategic option in conflict. When the risks outweigh the benefits of offensive action, states consider taking a more appropriate action, such as preparing the future battlefield using conventional warfare options along with the limited use of cyber warfare, given that the advantages of offensive actions in cyberspace have not yet outweighed the risks[32].

Cyberspace is an Anarchic System

James Adams views cyberspace as an anarchic system: "Cyberspace has become a new international battlefield." With no governing body or central authority, the Internet perfectly fits a real-world security model. In this model, each state stands alone or with its allies, whom it cannot fully trust, and is desperately trying to build up its cyber power and defenses while fearing that every penetration made by another state poses a direct threat to its security[33].

In this context, the Stuxnet cyber-attack was a security nightmare because it proves that any state is capable of attacking another state with impunity and without leaving any trace of the origin of the attack. Also, the neorealist theory predicts that there will be a complete breakdown of trust and of international institutions. As each state will fear imminent and unknown attacks, and consequently will retreat and build its own strength.

The lack of a hierarchical structure and overarching authority in cyberspace made many of the steps taken to hack and sabotage the centrifuges in Natanz possible. Cyberspace, as another arena in which states present their interests, and in which interests converge and collide, undoubtedly becomes an extension of the system intended by Waltz in his realistic analysis.

Balance of Power Analysis

Due to the relatively low cost of entering the field of cyber warfare, traditionally weaker states can challenge stronger states and redistribute powers in the system[34]. One of the most important direct results of the Stuxnet attack was the increasing sophistication of

[32] Collins, A. (Ed.). (2022). Contemporary security studies. Oxford university press.pp. 20-23.

[33] Adams, J. (2001). Virtual defense. Foreign Aff., 80, 98.pp 98-112.

[34] Langø, H. I. (2016). Competing academic approaches to cyber security. In Conflict in Cyber Space (pp. 23-42). Routledge.

Iranian cyber warfare capabilities and tactics[35]. Iran now possesses defense, deterrence and even cyber-attack tools that enabled it to target US and Israeli facilities and infrastructure networks. The reciprocal cyber-attacks between the two sides escalated after the Stuxnet attack, until analysts started calling it "cyber war" without hesitation.

Lindsay argues that only states with great technological powers have the ability to develop the most advanced cyber weapons suggesting that the asymmetric nature of the cyber domain may be overstated[36]. This may be reflected in the fact that Israel could not have developed Stuxnet alone without the help, financing and facilities of United States.

Stuxnet attack did not succeed in destroying all the centrifuges at the Natanz reactor. But if the goals were to bring a disruption or a delay to the Iranians' progress in uranium enrichment, it appears that Stuxnet was successful in achieving those realistic goals[37].

Conclusions

Realism, as a theory mostly concerned with issues of national security and power in international relations, is a very suitable theoretical framework for analyzing and understanding cyber-attacks. This analysis confirmed that realism is an appropriate framework for analyzing important issues related to security in cyberspace, and can provide useful insights into some of the enduring characteristics of international relations in cyberspace.

A realistic analysis of the Stuxnet cyber-attack was able to give us the following explanations:

1- The fact that United States and Israel joined forces to launch a powerful cyber-attack that could disrupt uranium enrichment at Iran's Natanz reactor. This cyber-attack was an attempt to maintain the relative power of two states over a third.

2- Cyberspace is a reflection of the anarchic international system in its structure, and therefore states are intertwined with interests forced to seek their own security. This was expressed as a direct action on the initiative of the two allies, United States and Israel, in the search for security and the realization of their interests using cyber force.

[35] Aitel, D. (2015). Iran Is Emerging as One of the Most Dangerous Cyber Threats to the US. [online] Business Insider. Available at: https://www.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-the-us-2015-12?r=US&IR=T [Accessed 1 Mar. 2022].

[36] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404.

[37] Avag, R. (2010). Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant? | Institute for Science and International Security. [online] isis-online.org. Available at: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ [Accessed 1 Mar. 2022].

3- The adoption of cyber-attack as a strategic option to maintain relative strength showed that cyber capabilities are an influential factor in the distribution of powers and capabilities in international relations. It can affect the relative power between states and ensure the survival of states in the international system.

4- The lack of a hierarchical structure and comprehensive authority in cyberspace, tempting governmental and non-governmental entities to use cyber-attacks to achieve their goals and interests.

5- Cyber-attacks are "unconventional weapons" that can ensure some balance to the anarchic international system, as no state can always be safe from cyber-attacks.

6- It is very difficult to track cyber-attacks in most of the cases, as the attackers can leave no trace or leave false evidence to implicate others.

Bibliography:

1. Nakashima, E. (2011). List of cyber-weapons Developed by Pentagon to Streamline Computer Warfare. The Washington Post. [online] 1 Jun. Available at: https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html [Accessed 28 Feb. 2022].
2. Fruhlinger, J. (2017). What Is Stuxnet, Who Created It and How Does It work? [online] CSO Online. Available at: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [Accessed 28 Feb. 2022].
3. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.
4. Eric Byres, P. (2011). Stuxnet Report: A System Attack. [online] ISSSource. Available at: https://isssource.com/stuxnet-report-a-system-attack/ [Accessed 28 Feb. 2022].
5. Langner, R. (2010). The Big Picture. [online] Langner Blog. Available at: https://www.langner.com/2010/11/the-big-picture/ [Accessed 28 Feb. 2022].
6. Langner, R. (2011). How to Hijack a Controller: Why Stuxnet Isn't Just about Siemens' PLCs. [online] Control Global. Available at: https://www.controlglobal.com/articles/2011/industrialcontrollers1101/ [Accessed 28 Feb. 2022].
7. Langner, R. (2013). To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group.
8. Broad, W.J. and Sanger, D.E. (2010). Worm Was Perfect for Sabotaging Centrifuges. The New York Times. [online] 19 Nov. Available at: https://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html [Accessed 28 Feb. 2022].
9. Zetter, K. (2011). Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant. [online] Wired. Available at: https://www.wired.com/2011/02/stuxnet-five-main-target/ [Accessed 28 Feb. 2022].
10. Nakashima, T.E. and E. (2010). Iran Struggling to Contain "foreign-made" "Stuxnet" Computer Virus. The Washington Post. [online] 28 Sep. Available at:

https://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html [Accessed 28 Feb. 2022].

11. Beaumont, P. (2010). Stuxnet Worm Heralds New Era of Global Cyberwar. [online] the Guardian. Available at: https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar [Accessed 28 Feb. 2022].
12. Sanger, D.E. (2012). Obama Order Sped up Wave of Cyberattacks against Iran. The New York Times. [online] 1 Jun. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [Accessed 28 Feb. 2022].
13. Halliday, J. (2010). Stuxnet Worm Is the "work of a National Government agency." The Guardian. [online] 24 Sep. Available at: https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency [Accessed 28 Feb. 2022].
14. Hounshell, B. (2010). 6 Mysteries about Stuxnet. [online] Foreign Policy. Available at: https://foreignpolicy.com/2010/09/27/6-mysteries-about-stuxnet/ [Accessed 28 Feb. 2022].
15. Markoff, J. (2010). Stuxnet Worm Is Remarkable for Its Lack of Subtlety. The New York Times. [online] 27 Sep. Available at: https://www.nytimes.com/2010/09/27/technology/27virus.html [Accessed 28 Feb. 2022].
16. Williams, D. (2009). Spymaster Sees Israel as World Cyberwar Leader. Reuters. [online] 15 Dec. Available at: https://www.reuters.com/article/idUSTRE5BE30920091215 [Accessed 28 Feb. 2022].
17. Williams, D. (2010). EXCLUSIVE - Cyber Takes Centre Stage in Israel's War Strategy. Reuters. [online] 28 Sep. Available at: https://www.reuters.com/article/idINIndia-51792020100928 [Accessed 28 Feb. 2022].
18. Williams, D. (2009). ANALYSIS-Wary of Naked force, Israelis Eye Cyberwar on Iran. Reuters. [online] 7 Jul. Available at: https://www.reuters.com/article/idUSLV83872 [Accessed 28 Feb. 2022].
19. The Economist (2010). A Worm in the Centrifuge. [online] The Economist. Available at: https://www.economist.com/international/2010/09/30/a-worm-in-the-centrifuge [Accessed 28 Feb. 2022].
20. Reals, T. (2010). Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes? [online] cbsnews.com. Available at: https://www.cbsnews.com/news/stuxnet-worm-a-us-cyber-attack-on-iran-nukes/ [Accessed 28 Feb. 2022].
21. Kelley, M.B. (2012). Obama Administration Admits Cyberattacks against Iran Are Part of Joint US-Israeli Offensive. [online] Business Insider. Available at: https://www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2012-6 [Accessed 28 Feb. 2022].
22. Halliday, J. (2011). WikiLeaks: US Advised to Sabotage Iran Nuclear Sites by German Thinktank. [online] The Guardian. Available at: https://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear [Accessed 28 Feb. 2022].

23. Sanger, D.E. (2009). U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site (Published 2009). The New York Times. [online] 10 Jan. Available at: https://www.nytimes.com/2009/01/11/washington/11iran.html [Accessed 28 Feb. 2022].
24. MacAskill, E. (2011). Stuxnet Cyberworm Heads off US Strike on Iran. [online] The Guardian. Available at: https://www.theguardian.com/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran [Accessed 28 Feb. 2022].
25. Sanger, D.E. (2010). Iran Fights Malware Attacking Computers. The New York Times. [online] 25 Sep. Available at: https://www.nytimes.com/2010/09/26/world/middleeast/26iran.html [Accessed 28 Feb. 2022].
26. Craig, A. (2013). Realism and Cyber Conflict: Security in the Digital Age. [online] E-International Relations. Available at: https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ [Accessed 1 Mar. 2022].
27. Reardon, R., & Choucri, N. (2012, April). The role of cyberspace in international relations: A view of the literature. In ISA Annual Convention, San Diego, CA (Vol. 1).
28. Collins, A. (Ed.). (2010). Contemporary security studies. Oxford university press.
29. Adams, J. (2001). Virtual defense. Foreign Aff., 80, 98.
30. Langø, H. I. (2016). Competing academic approaches to cyber security. In Conflict in Cyber Space (pp. 23-42). Routledge.
31. Aitel, D. (2015). Iran Is Emerging as One of the Most Dangerous Cyber Threats to the US. [online] Business Insider. Available at: https://www.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-the-us-2015-12?r=US&IR=T [Accessed 1 Mar. 2022].
32. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404.
33. Avag, R. (2010). Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant? | Institute for Science and International Security. [online] isis-online.org. Available at: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ [Accessed 1 Mar. 2022].