SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme

Mariusz Antoni Kamiński

m.kaminski@akademia.mil.pl

https://orcid.org/0000-0001-9395-9744

Faculty of National Security, War Studies University, gen. Chruściela "Montera" 103, 00-910 Warsaw, Poland

Abstract

The purpose of the article is to analyse Operation "Olympic Games" including, in particular, to indicate the political background to the activities aimed at preventing the development of Iran's nuclear programme, and to examine the preparation and conduct of the operation, the involvement of the US and Israeli intelligence services, and the use of intelligence methods and sources. An equally important objective is to indicate the real consequences of the cyberattack with the Stuxnet virus. In the research process, a critical analysis of literature in the field of Intelligence Studies and source materials (including legal acts, strategies, reports, and other official studies of the entities forming the US Intelligence Community) was carried out. The example of Operation Olympics Games shows that complex cyber-sabotage operations resulting in the destruction of critical infrastructure on a large scale require the involvement of numerous state resources and advanced cyber activities, and the use of many different methods and intelligence sources. Thus, strong states with well-developed intelligence capabilities are much more capable of effectively using cyber-sabotage on a large scale.

Keywords:

intelligence, Operation Olympic Games, Stuxnet, NSA, Unit 8200

Article info
Received: 3 December 2019
Revised: 30 April 2020
Accepted: 2 May 2020
Available online: 6 June 2020
DOI: http://doi.org/10.35467/sdq/121974

Introduction

A cyber-attack aimed at paralyzing critical infrastructure and causing physical harm is an increasingly common method of operation of intelligence agencies in different countries. The first such incident took place in 2010 when the Stuxnet computer virus caused the destruction of some 1,000 centrifuges used for uranium enrichment at the Natanz Iran underground facility. The attacks were attributed to the United States and Israel. Both countries thus wanted to halt or significantly delay Iran's nuclear programme. However, the use of the Stuxnet virus wasn't just another cyber-attack. In many ways, it was a pioneering act, as it was the first time that cybernetic tools were able to permanently destroy critical infrastructure assets. In order to achieve this, the United States and Israel used very large forces and resources in a joint operation called "Olympic Games."

The purpose of the article is to analyse Operation Olympic Games, including in particular to indicate the political background to the activities aimed at preventing the development of Iran's nuclear programme, and to present the preparation and conduct of the operation, the involvement of the US and Israeli intelligence services, and the use of intelligence methods and sources. An equally important objective is to indicate the real consequences of the cyberattack with the Stuxnet virus. This serves to verify the following working hypothesis: the example of Operation Olympics Games shows that complex cyber-sabotage operations resulting in the destruction of critical infrastructure on a large scale require the involvement of numerous state resources and advanced cyber activities, and the use of many different methods and intelligence sources. Strong states with well-developed intelligence capabilities are, therefore, much more capable of effectively using cyber-sabotage.

In the research process, a critical analysis of literature in the field of Intelligence studies and source materials (including legal acts, strategies, reports, and other official studies of the entities forming the US Intelligence Community) was carried out.

Political background

The issue of an effective proliferation policy, non-proliferation of weapons of mass destruction, is fundamental to the security of the United States and other Western countries. This is especially true for nuclear weapons. As Henry Kissinger emphasised, all Cold War American administrations were forced to plan their international strategies in the context of the frightening doctrine of deterrence, the awareness that a nuclear war could threaten our civilization. However, after the end of the Cold War, when more and more countries had atomic weapons, the doctrine became more ephemeral and deterrence less and less effective. It is difficult to determine who is deterring and at what price (Kissinger, 2017, pp. 154–155).

Samuel P. Huntington, on the other hand, pointed out that the United States has the capabilities to launch military intervention practically anywhere in the world. "These are the central elements of the military position of the United States as a global power and of the West as the dominant civilization in the world". However, if a country acquires a nuclear weapon, this potential worryingly evens out. Huntington gives the hypothetical example that "if Saddam Hussein had delayed his invasion of Kuwait for two or three years until Iraq had nuclear weapons, he would very likely be in possession of Kuwait and quite possibly the Saudi oil fields also" (Huntington, 1996, p. 186).

The United States is very concerned about the possibility of Iran acquiring nuclear weapons. A nuclear weapon in the hands of Iranian leaders could not only permanently disrupt

the already fragile stability in the Middle East and seriously endanger Israel's existence, but also affect the security situation throughout the world. President George W. Bush, in his annual State of the Union address on 29 January 2002, included Iran alongside Iraq and North Korea in the axis of evil. He pointed out that: "states like these, and their terrorist allies, constitute an axis of evil, arming to threaten the peace of the world. By seeking weapons of mass destruction, these regimes pose a grave and growing danger. They could provide these arms to terrorists, giving them the means to match their hatred. They could attack our allies or attempt to blackmail the United States. In any of these cases, the price of indifference would be catastrophic" (Bush, 2002).

Many strategic documents of the United States have also repeatedly pointed to the threat posed by Iran. The 2009 National Intelligence Strategy underlined that "Iran poses an array of challenges to U.S. security objectives in the Middle East and beyond because of its nuclear and missile programmes, support of terrorism, and provision of lethal aid to U.S. and Coalition adversaries" (National Intelligence Strategy of the United States of America, 2009).

Iran has for years consistently conducted research into the development of nuclear programs, arguing that it does so only for civilian purposes. However, the uranium enrichment programme, of which centrifuges were an essential part, was the key element. There was a lot of evidence suggesting that Iran had acquired large quantities of centrifuges and installed them at its Natanz facility, where two underground production halls with enough space for 50,000 centrifuges were built, and that by mid-2009, Iranians had installed around 8,000 centrifuges in one of the halls (Albright *et al.*, 2012, pp. 12–13).

Diplomatic pressure on Iran did not have the desired effect. The UN Security Council, in its Resolutions 1737 (2006), 1747 (2007), 1803 (2008), and 1835 (2008), called on Iran to suspend without delay certain activities that were sensitive from the standpoint of proliferation of nuclear weapons and imposed certain restrictive measures against it. However, Iran continued to develop its nuclear programme (Kelsey, 2017).

Due to the limited effectiveness of diplomatic measures and the subsequent economic sanctions, the United States began to seriously consider a bombing campaign against Iranian targets. As the former head of the National Security Agency Michael Hayden pointed out in his memoirs, the Pentagon's plans for various possible attacks were impressive. The plan was to conduct a lot of attacks to suppress the anti-aircraft defence before assault units would start raids on a large scattered and fortified target (Hayden, 2017, p. 340). Also, the Israeli authorities, in their assessment that Iran is very close to obtaining a nuclear weapon, put pressure on the US administration to bomb Iranian facilities. It should also be emphasised that in 2007 Israel carried out a bombing attack on a Syrian nuclear reactor in the Deir ez-Zor region as part of the Operation Outside the Box. However, in the case of Iran, such actions were much riskier. President George W. Bush later wrote in his autobiography that the military option had always been taken into account, but it was treated as the last resort (Bush, 2011, p. 488).

In addition, the case was complicated by the fact that in November 2007, the U.S. National Intelligence Estimate that was published contained a surprising statement that Iran had stopped its military nuclear programme in 2003. President G.W. Bush believed that the report not only undermined diplomacy, but also tied his hands on military action[1]. Robert Gates, on the other hand, the former head of the CIA, said that "the report had presented the evidence poorly, underemphasizing the importance of Iran's enrichment activity and overemphasising the suspension of a weapons-design effort that could easily be turned back on" (Sanger, 2009). There have also been opinions in the press that Israel

1. President G.W. Bush further indicated that he didn't know why the document was written like this. He suggested that perhaps the CIA tried so hard to avoid repeating the mistakes made in the case of Iraq that it underestimated the threat posed by Iran (Bush, 2011, pp. 488–491*).*

undermined the US report by providing credible information on the intensive development of Iran's nuclear programme. It was also suggested that in early 2008, Israel asked the US to provide a new generation of powerful bunker-busters capable of destroying underground facilities at Natanz and the right to fly over Iraq and refueling equipment so as to enable Israel's aircraft to attack Iranian facilities. The Americans refused. At the same time, Israel was offered the opportunity to participate in an operation which was supposed to slow down Iran's nuclear programme, including paralysing the country's industrial infrastructure and destabilizing the operation of centrifuges. The Americans had used various forms of sabotage before; for example, according to the media, the CIA used a family of Swiss engineers working with Iran to deliver defective power supply units, which caused an explosion at the Natanz facility and the destruction of about 50 centrifuges (Broad and Sanger, 2008). This time, however, the act of sabotage was to be on a much larger scale and involved the use of cyber-attacks.

Operation "Olympics Games"

The Stuxnet computer virus, which was used to conduct the cyberattack against Iran's objects in Natanz, first became known in June 2010, when it was identified by representatives of the Belarusian company VirusBlokAda. Afterwards, a lot was published on this subject[2]. Stuxnet was described, among other things, as the first malicious software (malware) designed specifically to attack a particular type of industrial control system (ICS) (Kerr, Rollins and Theohary, 2010, p. 1). However, as it turned out later, Stuxnet was a part of a large operation codenamed "Olympic Games," prepared jointly by the United States and Israel.

The first person to write about Operation Olympic Games was David Sanger, the author of a series of articles published in the New York Times[3] and then in the book "Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power" (Sanger, 2012a). Since then, public opinion has attributed the cybersabotage against the Iranian centre in Natanz to the American and Israeli agencies, although, of course, both countries have never officially admitted to these activities. This was due to the fact that the activity referred to as "covert action" meant the role of the state was not apparent or acknowledged publicly[4].

According to Sanger, the plan for the cyberattack against Iran's industrial infrastructure used in the nuclear programme was prepared in 2006 under President George W. Bush. Operation Olympics Games on the US side involved two major intelligence agencies: the National Security Agency (NSA) and the Central Intelligence Agency (CIA). The first task of the American agencies was to gather as much information as possible about the Natanz centre and the centrifuges used there. For this purpose, special software was used which was installed in computers of the German company Siemens, which together with an Iranian company supplied the equipment to the Natanz site. Thanks to the feedback that the programme sent to the NSA, US intelligence learned about the structure and the methods of operation of the Iranian facility (Sanger, 2012a, pp. 110–129).

The next step was to include the Israeli intelligence service within the framework of Operation Olympic Games, which had at its disposal important intelligence materials about the Natanz centre. At the same time, thanks to the NSA's cooperation with Israeli unit 8200, advanced work began on the development of an extremely complex computer virus that would paralyse the Iranian centrifuges. The result of the work of the NSA and unit 8200 was a computer worm called "the bug" by the Americans. To test its effectiveness, a virtual replica of the Natanz facility was built using P-1 centrifuges acquired in Libya in 2003, when Muammar al-Qaddafi had discontinued his coun-

2. The name of the virus, "W32.Stuxnet," was given by Symantec experts.

*3. Sanger indicates that "this account of the American and Israeli effort to undermine the Iranian nuclear programme is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the programme, as well as a range of outside experts. None would allow their names to be used because the effort remains highly classified, and parts of it continue to this day" (*Sanger, 2012b*).*

4. See: National Security Act of 1947 SEC. 503. [50 U.S.C. § 3093] "the term covert action means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."

try's nuclear programme. "Destructive testing" was conducted in several Department of Energy laboratories in the United States. The programme was probably also tested at Israel's Dimona nuclear facility. The tests were so successful that at the end of George W. Bush's term of office in 2008, the decision was made to use the virus to attack the Natanz centre (Sanger, 2012a, pp. 110–129).

However, it was not so easy to infect the facility with the virus. According to Sanger (2012b), the Americans and the Israelis used engineers and workers who had physical access to the equipment at the underground Natanz plant. They were either spies or people who were completely unaware, whose carelessness and recklessness were exploited. A USB flash drive was used to spread the first variants of the worm and at a later stage, more sophisticated methods of virus infection were developed.

Because Operation Olympics Games was only in its initial phase in 2008, President Bush, after his term of office ended, urged the new US President Barack Obama to continue his activities and President Obama issued an order to intensify the operation (Sanger, 2012b).

Following the disclosure of the Stuxnet virus, Albright *et al.* (2012, p. 15), who studied the development of Iran's nuclear programme, stated: "whichever nation launched that attack had a surprising amount of confidential detail about operations at the facility - far more inside information than could be acquired from IAEA reporting. Intelligence agencies needed to penetrate both the inner workings of that plant and a collection of Iranian companies, which illicitly obtained Siemens computer control equipment and software and prepared it for delivery to the centrifuge programme, leading to the Stuxnet attack".

Operation of the Stuxnet virus

According to the authors of the publication "White Paper. How Stuxnet Spreads - A Study of Infection Paths in Best Practice Systems," the Stuxnet is "a sophisticated piece of computer malware designed to sabotage industrial processes controlled by Siemens SIMATIC WinCC and PCS 7 control systems. The worm used both known and previously unknown vulnerabilities to install, infect and propagate, and was powerful enough to evade state-of-the-practice security technologies and procedures" (Byres, Ginter and Langill, 2001, p.1). The complex Stuxnet code was a self-replicating worm that attacked PLCs (Programmable Logic Controllers). PLCs are universal microprocessor devices dedicated to the control of manufacturing processes. They are part of industrial control systems architecture called SCADA (Supervisory Control and Data Acquisition). The main SCADA functions include collecting and visualising measurements, process control and alarming.

Of note is the fact that Stuxnet was an extremely precise programme. As Max Smeets emphasised, Stuxnet only affects a specified model of PLCs used in the Natanz facilities. If some computer system does not match the device characteristics, Stuxnet removes itself from the machine (Smeets, 2017, p. 24). Milevski (2011, p. 67), on the other hand, pointed out that Stuxnet's capacity to self-replicate, reproduce swiftly in the system, and disguise its presence until activated all indicate that it was created to make an unconventional attack on the Natanz facilities.

Stuxnet was designed to remain undetected for a long time and to consistently burden and degrade the centrifuges. In short, its operation meant that for a short time (about 15 minutes), the virus changed the frequency of rotation of the IR-1 centrifuges slightly above their safe speed, then it restored the normal state of operation (for ten to

twenty days), after which it slowed down the frequency of rotation of the centrifuges below the speed needed to enrich uranium (for about 50 minutes) and again returned to the normal state (for ten to twenty days). This sequence was constantly repeated (Lindsay, 2013). The employees of the plant in Natanz were, therefore, given the wrong information that the centrifuges were operating normally when, in fact, they were accelerating and slowing down.

According to Albright *et al.* (2012, p. 16), the operation of the Stuxnet virus caused the destruction of around 1,000 centrifuges at the Natanz site, which could have delayed Iran's nuclear programme by about 1 year.

Probably due to a bug in the new code version, Stuxnet got out of the Natanz centre and attacked over 100,000 computers worldwide (including Chevron's network in the USA). However, due to the fact that it was designed to attack specific devices in Iran, it did not cause much damage (Lindsay, 2013).

Consequences of Operation Olympic Games

Operation Olympic Games delayed Iran's nuclear programme by approximately one year, but did not completely stop it. Approximately 1,000 centrifuges (approximately 10% of the total number) were destroyed, but Iran quickly restored its resources and continued its programme. The real impact of the Stuxnet virus in stopping Iran from producing nuclear weapons has, therefore, proved to be relatively small.

However, the important question is whether, from the American perspective, the real goal of Operation Olympic Games was to halt the Iranian programme. M. Hayden's words seem to indicate that it was not, because the former head of the DNI and the CIA wrote that, in fact, everyone knew that whatever efforts were made, Iran's programme would only be slowed down and not stopped and Iran could be slowed down and punished but not stopped if it wanted to pay that price (Hayden, 2017, p. 340).

The act of cybersabotage committed using the Stuxnet virus achieved a different goal for the US administration: it enabled it to avoid bombing Iran and discouraged Israel from doing this by involving it in Operation Olympic Games. The use of cybernetic tools intended to attack the Natanz centre proved to be much less costly diplomatically. Interestingly, despite the disclosure of the fact that the US and Israel were behind the cyber-attacks on the Natanz facility, Iran did not use this to present itself as a victim of the attack and did not address a complaint to international institutions. Furthermore, it should also be emphasised that Israel did not limit its actions aimed at stopping Iran's nuclear programme to those carried out within the framework of Operation Olympics Games. Ján Kapusňak pointed out that Mossad was, among other things, responsible for the murder of scientists participating in Iran's programme and for a series of explosions in 2010-2013 at various Iranian nuclear facilities (including Fodo, Isfahan, Yazd, and others) (Kapusňak, 2013, pp. 380–381).

It seems that Operation Olympic Games could also have had a psychological effect and weakened the morale of Iranians. Albright *et al.* (2012, p. 15) even suggested in their report that this had brought Iran into a state of deep paranoia. Referring once again to the words of M. Hayden, one may have the impression that in a way, this was one of the objectives of the American-Israeli operation. As Hayden (2017, p. 345) wrote, what the Iranians create in Natanz is knowledge, technology, and self-confidence. Cyber-sabotage with the use of the Stuxnet virus was intended to undermine Iranian self-confidence. Also, as Valentin Weber further emphasised, in addition to having a deterrence effect,

Stuxnet caused Iranian authorities to doubt their ability to create a nuclear weapon (Weber, 2018, p. 246). D. Sanger (2012b) quoted one of the anonymous participants of Operation Olympic Games too, who allegedly said: "the intent was that the failures should make them feel they were stupid, which is what happened."

Conclusions

Operation Olympic Games was a precisely planned and sophisticated action of the American and Israeli intelligence agencies in cyberspace. For the first time, a computer virus was effectively used to attack critical infrastructure. This was made possible by the pooling of US and Israeli capabilities and intelligence. Such an operation required significant involvement of the state and cost a lot of money. Advanced solutions were used to test the Stuxnet virus in several laboratories of the US Department of Energy. Intelligence on the operation of the Iranian Natanz Centre also proved crucial. Although cybernetic tools were used for the main attack, the operation also involved other methods and intelligence sources such as signals intelligence (SIGINT), geospatial intelligence (GEOINT), and measurement and signature intelligence (MASINT). In order to infect the system at the Natanz centre with the virus, it was necessary to use human intelligence (HUMINT), i.e. to use spies who, having physical access to the underground plant, spread the first variants of the computer worm via an external USB memory stick. All of the above confirms that the example of Operation Olympic Games shows that complex cyber-sabotage operations resulting in the destruction of critical infrastructure on a large scale require the involvement of numerous state resources and advanced cyber activities, and the use of many different methods and intelligence sources. Thus, strong states with well-developed intelligence capabilities are much more capable of effectively using cyber-sabotage.

Nevertheless, several years after the discovery of the Stuxnet virus and the disclosure of information on Operation Olympic Games, it is clear that the activities of the US and Israeli intelligence agencies were a tactical success, but not a strategic one. They delayed Iran's nuclear programme but did not stop Iran permanently in its quest for nuclear weapons. Instead, they allowed the United States to avoid military action and bombardment of Iranian targets, while demonstrating to the Iranian people that they could not feel safe and that their nuclear programme would be sabotaged by various means, including cyber-sabotage. Later reports of another computer virus, Flame, which was to penetrate the Internet in the countries of the Middle East (e.g. record keyboard strikes, record conversations, activate microphones, and take screenshots) (Farwell and Rohozinski, 2012, p. 107) indicate that the United States will increasingly use cyberspace in its intelligence activities.

In many ways, the creation and use of the Stuxnet virus was a breakthrough. It was demonstrated for the first time that it is possible to permanently destroy critical infrastructure assets with cyber tools. Stuxnet damaged about 1,000 Iranian centrifuges and proved to be effective as a kinetic attack. Nevertheless, opinions that modern armed conflicts will move into cyberspace in the next few years seem to be very premature. This does not change the fact that attack and defense in cyberspace have now become a very important element supporting conventional military actions. Moreover, cyber-sabotage has become an increasingly common method of operation of intelligence agencies.

Funding

This research received no external funding.

Disclosure statement

No potential conflict of interest was reported by the authors.

References:

Albright, D., Brannan, P., Stricker, A., Walrond, C., and Wood, H. (2012) *Preventing Iran from getting nuclear weapons: constraining its future nuclear options*. New York: The Institute for Science and International Security.

Broad, W. J. and Sanger, D. E. (2008) 'In Nuclear Net's Undoing, a Web of Shadowy Deals', *New York Times*. Available from: http://www.nytimes.com/2008/08/25/world/25nuke.html (Accessed 30 November 2019).

Brown, G. D. (2011) 'Why Iran Didn't Admit Stuxnet Was an Attack', *Joint Force Quarterly*, (63)4.

Bush, G. W. (2002) 'The President's State of the Union Address', Available at: https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html (Accessed: 30 November 2019).

Bush, G. W. (2011) *Decision Points.* New York: Crown Publishing Group.

Byres, E., Ginter, A. and Langill, J. (2001) *White Paper. How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems.* Tofino Security, Abterra Technologies, ScadaHacker.com.

Farwell, J. P., Rohozinski, R. (2012) 'The New Reality of Cyber War', *Survival: Global Politics and Strategy*, (54)4.

Hayden, M. V. (2016) *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Book.

Huntington, S. P. (1996) *Clash of civilizations and the remaking World Order*. New York: Simon and Schuster.

Kapusňak, J. (2013) 'Covert operations attributed to Israel's Intelligence Services against Iran's nuclear program' in Majer, M., Ondrejcsák, R., Tarasovič V., and Valášek, T. (eds.) *Panorama of Global Security Environment, Centre for European and North Atlantic Affairs*, Bratislava: Centre for European and North Affairs.

Kelsey, D. (2017) *UN Security Council Resolutions on Iran*. Available at: https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran (Accessed: 30 November 2019).

Kerr, P. K., Rollins, J. and Theohary, C. A. (2010) *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Washington: Congressional Research Service.

Kissinger, H. (2017) *World order*. New York: Penguin Press.

Lindsay, J. R. (2013) 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, (22)3.

Milevski, L. (2011) 'Stuxnet and Strategy: A Special Operation in Cyberspace?', *Joint Force Quarterly*, (63)4.

National Intelligence Strategy of the United States of America (2009) Available at: http://fas.org/irp/offdocs/nis2009.pdf (Accessed: 30 November 2019).

Osawa, J. (2017) 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem', *Asia-Pacific Review*, (24)2.

Prince, B. (2010) *Defense Department Confirms Critical Cyber-attack*. Available at: http://www.eweek.com/security/defense-department-confirms-critical-cyber-attack (Accessed: 30 November 2019).

Sanger, D. E. (2009) 'U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site', *New York Times*. Available at: http://www.nytimes.com/2009/01/11/washington/11iran.html (Accessed: 30 November 2019).

Sanger, D. E. (2012a) *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*. New York: Random House.

Sanger, D. E. (2012b) 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *New York Times* Available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (Accessed: 30 November 2019).

Segal, A. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs.

Smeets, M. (2017) 'A matter of time: On the transitory nature of cyberweapons', *Journal of Strategic Studies,* (41)1–2.

Veebel, V. and Ploom, I. (2016) 'Estonian Perceptions of Security: Not Only About Russia and the Refugees', *Journal on Baltic Security*, (2)2.

Weber, V. (2018) 'Linking cyber strategy with grand strategy: the case of the United States', *Journal of Cyber Policy*, (3)2.