Stuxnet as Cyber-Enabled Sanctions Enforcement

Panayotis A Yannakogeorgos
Air Force Cyber College
Maxwell AFB

Eneken Tikk
International Institute for Strategic Studies

Abstract - Our re-reinterpretation of Stuxnet to connect the dot between geopolitics and technology tell a different story with a secondary set of lessons. We believe Stuxnet deserves a broader legal and political analysis for the purposes of critical thinking about how cyberspace is used to achieve international security objectives from legal and political angles. In particular, we seek to address a gap in the literature, asking whether the worm was authorized under article 41 of the UN charter as a sanctions enforcement tool through an interpretation of UNSC resolutions and related documents of the International Atomic Energy Agency (IAEA). If such authorization exists (and we believe it might), Stuxnet would qualify as a lawful action under international law, targeting Iran's nuclear equipment and software pursuant to international sanctions.

Keywords — cyber statecraft, national security, nuclear weapons, Stuxnet

Introduction

I. Introduction

Cyber statecraft is a relatively non-transparent instrument of national power. Norms of state behavior are formed on the basis of state practice. The opaque policy processes involved in authorizing the use of cyber tools to achieve strategic interests do not offer many case studies on which to interpret states use of cyberpower to develop norms of responsible state behavior. As a landmark example of politically motivated cyber attacks that have received systematic political attention since 2007, Stuxnet has become the textbook case of an armed attack achieved by cyber means. Legal and political scholars have been divided on the point that malware planted in the Iranian nuclear plant in Natanz is a use of force via cyberspace satisfying the criteria of Article 2 (4) of the UN Charter.[i] Indeed, one strong statement characterizes Stuxnet as "in addition to violating the general prohibition against a use of force against another nation, this event arguably violated the law of war."[ii] Others see parallels between the malicious software to the use of nuclear weapons on Hiroshima and Nagasaki.[iii]

This paper challenges these assumptions that Stuxnet qualified as a use of force and, in doing so, explores alternative ways to examine its international legality. We propose an alternative analysis: Iran had obligations it assumed to abide by United Nations Security Council (UNSC) Chapter VII resolutions; it choose not to, and the UNSC pursued its rights under the Charter to coerce it to do so via sanctions against the entire socio-technical substrate of its nuclear program.

This is an academic article written for the policy community, and the authors have neither access to the malware nor an ability to reverse engineer it to assess its technical sophistication. Our key assumption is that the software was programmed to exploit vulnerabilities in the functional design of the instrumentation and process control systems of industrial control systems (ICS) specifically within Iran's illicit nuclear program to disrupt the communications between sensors and operators to a degree that physical damage was caused (but not significant damage such as a nuclear meltdown).[iv] Although the malware spread globally, its distribution did not generate physical damage in non-targeted systems. Its global distribution and inert nature when it was resident on non-targeted systems indicates that it was very specific tool. As such, we believe those advancing the technical conclusion of Stuxnet constituting a forceful intervention on the premise that the computer code had a physical effect may have failed to consider its authors were operating under a broader set of normative caveats. These include the possibility of a political decision to use a software tool to disrupt the illicit nuclear infrastructure of a country the UN Security Council recognized could be pursuing a militarized nuclear weapons program, and had mandated sanctions against Iran's nuclear program in an attempt to disrupt progress. Thus, the authors seek to use the Stuxnet case fuse academic theory and international relations for the purpose of extending the basis of critical thinking about policy-relevant academic research.

II. Connecting the Dots Between Geopolitics & Technology

Cyber statecraft is still a rare skill among countries believed to possess military cyber capabilities. A study by the UN Institute for Disarmament Research indicated that "32 states included cyberwarfare in their military planning and organizations, while 36 states had civilian agencies charged with a domestic cybersecurity mission.[v] That Stuxnet was a state-sponsored attack, while not conclusive, is difficult to dispute. The complexity of the software, engineering, and cryptography, is something that only a state sponsor could

develop.[vi] Without evidence combining circumstantial political will and technological capacity by states, and in the absence of relevant procedural initiative, attributing Stuxnet to a specific state actor is not an option without voluntary attribution.[vii] For the purposes of this discussion, the authors presume that Stuxnet was a state actor operation.

The authors of this article have chosen to test Stuxnet as an example of pursuit of nation-states' national interests. Our main interest is not to point the finger at a particular nation-state, but to examine the possible legal analysis that may have gone into the operation in the course of its preparation and planning. With due respect to critiques of academic over-complexification of foreign policy strategies and outcomes, the authors of this article find it difficult to accept that Stuxnet was designed as a tool of aggressive force, and the fact that it might be perceived as such was likely not easily dismissed in the political judgment of its planners. The standard of the threat or use of force is unclear when it comes to destruction, and scholarly reactions would have been easily predictable. This is further supported by the technology of the worm. Its aim was to delay an illicit nuclear program for an extended period of time, not to destroy it entirely. Finally, the response of Iran, which had otherwise been relatively defensive against political and economic sanctions imposed on it, chose to remain silent is another indicator Stuxnet not having crossed over internationally accepted thresholds of the use of force.[viii] One could argue that the US may have regarded this as a use of force if it had targeted US critical infrastructure. However, the US is not under any UN sanctions. If all these assumptions are true – this informs development of possible global norms of responsible state behavior in cyberspace by outlining the standards of legal and political analysis to be invested into planning and preparing, but also assessing a cyber incident that already occurred.

In order to invoke new thought we avoid over-exploited terms such as "cyberweapon" and go beyond the analysis of UN Charter 2(4) even though we need to mention both. Arguments that Stuxnet a peacetime act of cyberwar reason is that because Stuxnet created physical effects that damaged or destroyed physical objects, it amounts to a use of force.[ix] It is our belief that the novelty of computer code creating physical effects that damaged nuclear centrifuges has overwhelmed the debate today. The focus of our argument is not whether or not Stuxnet was or was not a weapon as more consideration of the geopolitical context in which the tool was utilized is required. Stuxnet is analyzed here through the lens that it is a software program with modules designed to disrupt communications in the control systems of nuclear centrifuges deemed a nuclear proliferation risk by the IAEA. The UNSC placed sanctions on Iran in order to dissuade it from further use of those reactors until Iran could prove without reasonable doubt that its nuclear program was indeed for peaceful purposes such as medical research and energy production. Iran continued to flout UN Security Council resolutions (UNSCR) by not suspending all proliferation sensitive nuclear activities, to gain IAEA inspectors' confidence in its nuclear program.

Issues of sovereignty and international obligations to maintain peace and security are important here. Often invoked in the analysis of Stuxnet, Article 2, chapter 4, the UN charter states that member states must: "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations." Boxing in the interpretation of Stuxnet only within the context of 2(4) takes the event out of the broader techno-geopolitical context.

That the charter also constrains states from unilateral recourse, except in self- defense to the use of force, is indisputable. Also indisputable is that there has been an inherent tension between the defense of humanity and the defense of sovereignty. However, the principle of sovereignty is not permanent. It is not unprecedented for the UN Security Council to compromise sovereignty when it considers threats to international peace and security as more pressing pursuant to Art. 39. The responses to these situations include both Art. 41 and 42 (but they can only apply after an Art. 39 finding). The Security Council may determine that maintaining a particular nation-state's sovereignty would elevate the risks to international stability and security to such an extent that the Council decides to take collective measures under Chapter seven of the UN Charter. This does not imply that the UNSC has the authority to deprive a nation-state of sovereignty. Instead, Council actions can allow for suspension of the non-interference principle and the piercing of a nation's sovereignty for purposes deemed legitimate by the Security Council. Otherwise, the state still maintains its sovereignty. At this point, States can invoke an exception to Art. 2(4) under other Charter terms. Art. 41 measures only authorize non-use of force means, which means states, are still obligated by Art. 2(4) when acting pursuant to Art. 41. This is exactly the circumstances that existed between Iran and the international community when Stuxnet was discovered.

The portions of Charter dealing with sanctions and sanctions enforcement thus become more relevant to the Stuxnet case. Article 2(5) of the Charter articulates that "All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United

Nations is taking preventive or enforcement action." Preventative or enforcement action in the Security Council can only take place after a UN Security Council resolution passes with a unanimous vote of the five permanent members of the Council. Under chapter 7(art. 41) the Security Council may take measures short of the use of armed force to achieve: "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations." As Iran was under preventative Security Council action, and Stuxnet interrupted communications between machine and humans controlling processes an illegal nuclear program, the action cannot be quickly discounted as an aggressive use of force. Rather, it could be considered as a tool of disruption enforcing sanctions and upholding nuclear nonproliferation regimes.

The UN Security Council has a decades-long history of being consistent on the matter of arms control and disarmament to prevent proliferation of all weapons of mass destruction. Iran was under an IAEA inspection regime due to concerns that it was not fulfilling its duties under Article IV of the Treaty on the Non Proliferation of Nuclear Weapons to not develop a military nuclear weapons program. Indeed, in the time period between 2002-2006, Iran had not gained the confidence of IAEA that Iran's nuclear program was solely being used to develop, research, produce and use nuclear energy for peaceful purposes. This was due to Iran's history of concealment of nuclear activities since September 2002. This concealment, in combination with the discovery of technological processes related to the fabrication of nuclear weapons, placed the Iranian nuclear program into the box of being a threat to international peace and security.[x]

Even with this history, in November 2005, the IAEA had discovered Iranian documents related to the procedures of casting uranium metal into hemispherical form- an indicator of research to create nuclear weapons. As such, in 2006 the IAEA called on Iran to "re-establish full and sustained suspension of all enrichment-related and reprocessing activities, including research and development" for verification by the IAEA.[xi]

Events at the IAEA Board of Governors led to several meetings of the UNSC over the course of that year. The UNSC issued a resolution in December 2006 "to constrain Iran's development of sensitive technologies in support of its nuclear and missile programmes."[xii] After IAEA's acknowledgement of their inability to confirm that Iran was not pursuing undeclared nuclear activities, the Security Council adopted a resolution in June 2006 demanding that Iran suspend all uranium enrichment programs. Tehran's failure to comply resulted in the Council imposing sanctions on Iran's trade in sensitive nuclear materials and technology in December 2006.[xiii] Following the IAEA's further unsuccessful mitigation attempts, the Security Council passed Resolution 1747 in March 2007. These expanded the 2006 sanctions while also naming specific officials as targets of the sanctions and adding additional sanctions against Iranian financial institutions.

On the basis of this very abridged history, Iran did not have the freedom to control its nuclear program as it was under UNSC sanctions. As such, it was fair game for states to comply with their international obligations to prevent the proliferation of nuclear weapons in Iran.

Deep reading into the UNSCR makes it clear that the purpose and intent of the sanctions were to degrade Iran's nuclear capability by limiting its access to technology. Under operative paragraph 5 of UNSCR 1696 which called "upon all States, in accordance with their national legal authorities and legislation and consistent with international law, to exercise vigilance and prevent the transfer of any items, materials, goods and technology that could contribute to Iran's enrichment-related and reprocessing activities and ballistic missile programmes." Thus, the question is really whether UNSCR 1737 contains authorization that might be read to include Stuxnet. Reading UNSCR 1737, it is explicitly stated that: "all States shall take the necessary measures to prevent the supply, sale or transfer directly or indirectly from their territories, or by their nationals or using their flag vessels or aircraft to, or for the use in or benefit of, Iran, and whether or not originating in their territories, of all items, materials, equipment, goods and technology which could contribute to Iran's enrichment-related, reprocessing or heavy water-related activities, or to the development of nuclear weapon delivery systems."[xiv] The operative words, with an emphasis here on the technology, to "indirectly" take action and prevent the use in Iran provides evidence of the international communities intent to suspend Iran's sovereignty over materials, equipment and technology that was involved in the sanctioned nuclear program**.** Further in operative paragraph 4a-c, individual states are to determine whether or not a particular technology would "contribute to enrichment-related, reprocessing or heavy water-related activities, or to the development of nuclear weapon delivery systems."

Since Stuxnet targeted process control systems embedded in technology that was under sanction to prevent Iran from procuring and using any items, materials, goods and technology related to its nuclear program including software specially designed for the use of centrifuges, we then have to consider the extent to which the programmers intended their software to be used as a tool of technological disruption rather than destruction. This leads to certain misperceptions that Stuxnet was a unitary computer worm that aimed to cause centrifuges to blow up. Ralph Langer in "To Kill a Centrifuge" describes two different variants of Stuxnet: the first version of Stuxnet sought to overpressure the centrifuges (S7-417 controllers) and the second version sought to increase the rotor velocity in the centrifuge drive system. Both version of the malware created a situation in which the system was being degraded, but data still flowed from the sensor to Iranian system operators showing that everything was

functioning properly.[xv] The end result was not the destruction for the nuclear facility, but the spoilage and delay of the production of highly enriched uranium due to the human operators receiving disrupted communications from sensors.[xvi] In the later version of the software, the worm blocked control code from execution causing the centrifuges to overspeed or transition through critical speeds.[xvii]

As has been documented, the technical sophistication of the malware is evidence of a team that had "The detailed pin-point manipulations of these sub-controllers indicate a deep physical and functional knowledge of the target environment; whoever provided the required intelligence may as well know the favorite pizza toppings of the local head of engineering."[xviii] Further, it has been noted that Stuxnet programmers were "in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead. This is interesting in that Stuxnet could have been executed at a level that equals a use of force, but it wasn't. However, since it may have been able to execute functions to cause worse damage, then it seems plausible to argue it constituted a "threat" to use force which is prohibited equally under Art. 2(4) as an actual use of force. This undercuts the arguments that it was merely a continuation of economic sanctions by non-violent means. This is where author intentionality becomes an important point to consider. The threat of a use of force was never implied in the execution of the tool, and the victims could only have known about the "threat" of the use of force after discovery and careful analysis of the complex malicious software. Furthermore, there was never any state that claimed responsibility, and followed on with threats to the virus to presume this cyber enabled tool to be a threat of the use of force.[xix]

Therefore, Stuxnet is a low-yield cyber tool with the overall intention to reduce the lifetime of Iran's centrifuges and make their fancy control systems appear beyond their understanding."[xx] That they chose not to demonstrates the intent to disrupt the data flows on which humans relied to ensure the proper functioning of the centrifuges. The result was damaged centrifuges, and a delayed nuclear program rather than the destruction of the nuclear centrifuges on a scale of a bombardment that might cross the use of force threshold. Furthermore, there is a question as to the directness of the effects. A use of force is often treated as such because the violence/damage is so directly linked to the means and method used; whereas are there intermediate steps in the chain of causation between cutting off food and/or money and people starving. They may both end with violence, but the law treats them differently. The tricky thing about Stuxnet is that it lies in between the two prior cases – it did have immediate, direct physical effects that equate to the bomb landing where you intended, but those effects were not as destructive as a bomb.

Overall, the intent of the sanctions against Iran were not to sweep across and punish Iranian society. In the case of Iraq's UN sanctions, the common Iraqi people had paid a harsh physical price after a decade of sanctions. Kofi Annan, then UN Secretary General understood this, and early in his tenure declared that sanctions need refining if they are to be seen as more than a figleaf in the future. Hence, the recent emphasis on targeted sanctions which prevent the travel, or freeze the foreign bank accounts, of individuals or classes of individuals -- the so-called "smart sanctions." Annan further stated that targeted sanctions require: "on the part of the Security Council and Member States, a willingness not only to tackle technical operational questions, but also the broader political questions of how best we ensure the fullest and broadest compliance with the will of the international community on the part of recalcitrant States."[xxi] As the UN system evolved towards a norm of targeted sanctions regime, including at the technical and operational level, Stuxnet begins to look more like a sanctions enforcement tool rather than a unilateral use of force. Examining what experts believe actually happened at the technological level assists in refining the geopolitical context of Stuxnet.

Stuxnet was primarily designed to disrupt or interrupt the electronic communications between a programmable logic controller and human-machine interface in a nuclear process control system. Arguments claiming Stuxnet was an armed attack focus on the cyber-physical connection, claiming that the effect was the same as a use of force. However, even with economic sanction or the interruption of any means of communication, there are always be a secondary effect of death or property damage that are not equated with a use of force. Iraq and North Korea's history under sanctions is evidence of this. However, economic sanctions that result in starvation are not considered "armed attacks" but the consequences of sanctions enforcement. Stuxnet was thus not a use of force, but rather another tool of sanctions enforcement specifically designed to disrupt a nuclear program presenting proliferation risks and constituting a threat to international peace and security.

Some observers suggest that since Iran was a victim of a cyber attack, then Iran has had a right to response. Indeed, since 2010 when Stuxnet was revealed, Iran has been more active on the cyber statecraft front. Allegedly conducting distributed denial of service attacks against US financial institutions and destroying data on Saudi Aramco's business networks are but two examples of Iran's aggressiveness in cyberspace. Interpreting Stuxnet as illegal under 2(4) opens the window that any Iranian action against the United States is a potentially legal retorsion. Even if Stuxnet provided Iran with the opportunity to claim that it had been subjected to a use of force, its right to respond in self-defense would be limited by the principle of immediacy, preventing it from being able to claim the right of self-defense years following the attack. Some see this as a natural escalation post Stuxnet.

III. Conclusions

What is clear is that the UN Security Council had not anticipated the use of cyber means to disrupt the technology being used. This opens up a broader debate on Article 41 authority for cyber enabled sanctions short of the use of force, namely the extent to which "interrupting communications" within technologies controlling processes targeted by UN sanctions. Stuxnet certainly created mainstream awareness of the interdependence between physical platforms and cyberspace, and the ability of software to trigger effects in control systems to produce effects in the physical world. However, within the above interpretation, it would not rise to either an armed attack, but something akin to the equivalent of a prevention of use of equipment prohibited in a nations territory pursuant to the UN's collective security system. If targeted interventions utilizing cyber means are too loosely labeled as uses of force, the concept loses its meaning in the development of statecraft. The basis for this interpretation rests with the UNSC sanctions Iran faced in 2006. Therefore, context of the UN sanctions created legally more favorable conditions for Stuxnet to fun ction as a mechanism of cyber enabled sanctions enforcement.

References

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first ..."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

---

[i] Foltz, Andrew C. "Stuxnet," Schmitt Analysis," and the Cyber" use of Force" Debate." *Joint Force Quarterly* 67, no. 4 (2012): 40-48.

[ii] Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." Joint Force Quarterly 63 (2011): 70.

[iii] Kennette Benedict, ''Stuxnet and the Bomb,'' *The Bulletin of the Atomic Scientists*, 15 June 2012, Bhttp://thebulletin.org/stuxnet-and-bomb

[iv] Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." Security & Privacy, IEEE 9, no. 3 (2011): 49-51.

Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from stuxnet." Computer 44, no. 4 (2011): 91-93.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. "Stuxnet under the microscope." ESET LLC (September 2010) (2010).

Kushner, David. "The real story of Stuxnet." *Spectrum, IEEE* 50, no. 3 (2013): 48-53.

[v] United Nations Institute for Disarmament Research *The Cyber Index: International Security Trends and Realities* http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

[vi] Lewis, James A. "Cybersecurity: Assessing the Immediate Threat to the United States." *Center for Strategic and International Studies, Statement before the House Oversight and Government Reform Committee, Subcommittee on National Security, Homeland Defense, and Foreign Operations, csis. org/testimony/cybersecurity-assessing-immediate-threat-united-states* (2011).

Broad, William J., John Markoff, and David E. Sanger. "Israeli test on worm called crucial in Iran nuclear delay." *New York Times* 15 (2011): 2011.

[vii] Panayotis A Yannakogeorgos, "Was Russia Behind Stuxnet?" in *The Diplomat* (10 December 2011) http://thediplomat.com/2011/12/was-russia-behind-stuxnet/

[viii] Statement by HE Dr Hassan Rouhan to the 69th Session of the UN General Assembly (23 September 2014) http://www.un.org/en/ga/69/meetings/gadebate/pdf/IR_en.pdf

[ix] Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" Joint Force Quarterly 63 (4th Quarter 2011), 64;

[x] IAEA Board of Governors Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran Resolution GOV/2006/14 (4 February 2006)

[xi] International Atomic Energy Agency "Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran" Resolution GOV/2006/14) Page 2

[xii] UNSC, Resolution 1737 (2006) 2.

[xiii] IAEA, Communications Received from Certain Member States Regarding Guidelines for the Export of Nuclear Material, Equipment and Technology

[xiv] UNSCR 1737 Operative Paragraph 3

[xv] Langner, Ralph. "To kill a centrifuge." *The Langner Group, http://www. langner. com/en/wp-content/uploads/2013/11/To-kill-acentrifuge. pdf, Tech. Rep* (2013)13.

[xvi] Lüders S. Stuxnet and the impact on accelerator control systems. Proceedings of ICALEPCS2011, Grenoble, France. 2011 Oct:1285-8.

[xvii] Langner, 14

[xviii] Langner, 10.

[xix] Note, the right of self-defense is in response to an "armed attack" which not everyone equates with a use of force (the idea being that more than a mere use of force (shooting a bullet across a border) is required to constitute an armed attack giving rise to self-defense rights. The US doesn't see this distinction as relevant, but is in the minority. I'd think you'd want to at least note the variation in views.

[xx] Langner, 15

[xxi] SECRETARY-GENERAL REVIEWS LESSONS LEARNED DURING "SANCTIONS DECADE" IN REMARKS TO INTERNATIONAL PEACE ACADEMY SEMINAR. http://www.un.org/press/en/2000/20000417.sgsm7360.doc.html