A. Obama Order Sped Up Wave of Cyberattacks Against Iran

Case prepared in 2015 by Ms. Margherita D'Ascanio, LL.M., student at the Geneva Academy of International Humanitarian Law and Human Rights, under the supervision of Professor Marco Sassòli and Ms. Yvette Issar, research assistant, both at the University of Geneva.

N.B. As per the disclaimer, neither the ICRC nor the authors can be identified with the opinions expressed in the Cases and Documents. Some cases even come to solutions that clearly violate IHL. They are nevertheless worthy of discussion, if only to raise a challenge to display more humanity in armed conflicts. **Similarly, in some of the texts used in the case studies, the facts may not always be proven;** nevertheless, they have been selected because they highlight interesting IHL issues and are thus published for didactic purposes.

[**Source:** 'Obama Order Sped Up Wave of Cyberattacks Against Iran', The New York Times, 1 June 2012, available at: http://www.nytimes.com]

[1] WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.
[2] Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.
[…]
[3] Told it was unclear how much the Iranians knew about the code, […] Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.
[…]
[4] The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. […]

[5] It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.
[…]
[6] Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. […]

A Bush Initiative

[7] The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America's European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation's nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.
[8] Iran's president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.
[…]
[9] […] General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, […] joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.
[10] The goal was to gain access to the Natanz plant's industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.
[11] The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to

map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. […]

Breakthrough, Aided by Israel

[…]
[12] Then the N.S.A. and a secret Israeli unit respected by American intelligence officials for its cyberskills set to work developing the enormously complex computer worm that would become the attacker from within.
[…]
[13] When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed “destructive testing,” essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department’s national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.
[14] Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. […] The worm was declared ready to test against the real target: Iran’s underground enrichment plant.
[15] “Previous cyberattacks had effects limited to other computers,” Michael V. Hayden, the former chief of the C.I.A., said […]. “This is the first attack of a major nature in which a cyberattack was used to effect physical destruction,” rather than just slow another computer, or hack into it to steal data.

“Somebody crossed the Rubicon,” he said.

[…]
[16] The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. “The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence,” one of the architects of the early attack said.
[17] The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. “This may have been the most brilliant part of the code,” one American official said.
[…]
[18] But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. […]

[19] Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure […].
[20] What he did not say then was that he was also learning the arts of cyberwar. […] Mr. Obama authorized the attacks to continue […].
[21] But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. […]
[22] An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.
[23] "We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."
[…]
[24] The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself "in the wild" […].
[25] "I don't think we have enough information," Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran's oil revenues.
[26] Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.
[…]

B. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?

[**Source:** 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?', Institute for Science and International Security, 22 December 2010. Available at: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ Footnotes omitted]

[…]
[1] In late 2009 or early 2010, Iran decommissioned and replaced about 1,000 IR-1 centrifuges in the Fuel Enrichment Plant (FEP) at Natanz, implying that these centrifuges broke. Iran's IR-1 centrifuges often break, yet this level of breakage exceeded expectations and occurred during an extended period of relatively poor centrifuge performance.
[2] […] If Stuxnet's goal was the destruction of all the centrifuges in the FEP, Stuxnet failed. But if its goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating FEP while

making detection of the malware difficult, it may have succeeded, at least for a while.

Iranian Statements

[3] Although Iran has not admitted that Stuxnet attacked the Natanz centrifuge plant, it has acknowledged that its nuclear sites were subject to cyber attacks. President Mahmoud Ahmadinejad recently admitted that a software attack affected Iran's centrifuges. "They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts," he told reporters at a media conference.
[4] The timing of the removal of about 1,000 centrifuges is consistent with another Iranian official's statement of when Iran suffered a cyber attack. On November 23, 2010, Ali Akbar Salehi, then head of Iran's Atomic Energy Organization and current acting foreign minister, confirmed to IRNA that malware had indeed reached Iran: "One year and several months ago, Westerners sent a virus to [our] country's nuclear sites."
[…]

Ambiguity about Stuxnet's Attack Sequences

[7] The specific goals of Stuxnet's attacks are not fully understood. Likewise, very little is known about the actual progression of each attack and the FEP's counter-measures to an attack. But Stuxnet at a minimum appears intended to disrupt operations and increase the number of centrifuges that fail while carefully disguising the malware's presence from the operator. To that end, each attack sequence sends commands to shut off the frequency converters' warning and safety controls aimed at alerting operators of the speed up or slow down.
[…]
[8] Based on Symantec's deciphering of infection sequence A, which is the attack involving a preponderance of Finnish frequency converters, Stuxnet can destroy centrifuges. In sequence A, there are two specific attacks that are separated by about a month. The first, called sequence one, would raise the speed of the centrifuge as high as a frequency of 1,410 Hz during a 15 minute attack, before the malware returns the control system to normal operation. After waiting about 27 days, Stuxnet would launch attack sequence two. The first part of this attack would lower the frequency toward 2 Hz and last 50 minutes. The second part would raise the frequency back to the nominal frequency of 1,064 Hz. After another 27 days, the first attack sequence would start again; followed by sequence two 27 days after that.
[9] However, Stuxnet's effects may also be more subtle, disrupting operations without destroying all the centrifuges in the plant. For example, the time for an attack is limited. During the fifteen minute attack that raises the frequency to 1,410 Hz, the motor (or the centrifuge) may not reach this maximum frequency that would guarantee its destruction. The attack appears to end before this maximum is obtained, although the speeds achieved are so great that destruction may be guaranteed in any case. In the attack that lowers the frequency to a minimum of 2 Hz, the slowdown time may be so long that the frequency can be reduced by less than 200 Hz before the attack ends. […]

Post-Event Impact

[11] […] However, it remains unclear when Iran learned the FEP could be under cyber attack, and whether its computers and control systems at Natanz are now clear of Stuxnet. […]

Conclusion

[12] Although Stuxnet is a reasonable explanation for the apparent damage to module A26, questions remain about this conclusion. The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. But still unknown are parts of the attack sequences and possible responses by the FEP control system. These responses could act during the attack to reduce the magnitude of the change in frequency or otherwise act to protect the centrifuges. […]

A Final Concern

[13] For many years, governments have pursued methods to disrupt Iran's ability to procure goods illegally overseas for its nuclear programs, particularly its gas centrifuge program. Such overt and covert disruption activities have had significant effect in slowing Iran's centrifuge program, while causing minimal collateral damage. In contrast to overt military strikes, there is an appeal to cyber attacks aimed at a centrifuge plant built with illegally obtained, foreign equipment, and operating in defiance of United Nations Security Council resolutions. However, Stuxnet appears to have spread unintentionally and well beyond its targets. Part of the reason is in the design of Stuxnet, which needs to spread in order to increase its chance of infecting an industrial control system via a removable drive used with an infected computer.
[…]

Discussion

I. General questions

1. (Document A, paras. 1 - 8, 10, 12 - 15, 22 – 24; Document B, paras. 1, 2, 7 – 10, 12-13)
    a. (Document A, paras. 1 – 3, 5- 8, 10, 15 – 16, 22 – 24; Document B, paras. 1, 2, 7 – 10, 12 – 13) What distinguishes "Stuxnet" from other viruses? How did it work? What was its purpose? What were its effects?
    b. (Document A, paras. 1 – 4, 7 – 8, 12 – 15; Document B, para. 13) What was to be gained from damaging and destroying the Iranian centrifuges? Who was responsible for the damage and destruction of the Iranian centrifuges? Is attribution under public international law a necessary precondition for an analysis of whether IHL applies?

II. Qualification of the situation

1. (Document A, 1, 2, 10, 11, 21 – 23; Document B, 2, 10, 12, 13)

a. Does IHL apply in the present case? If so, could you classify the conflict? In this case, did an armed attack in the sense of the UN Charter occur? Was the attack an act of violence covered by P I, Art. 49?
b. With respect to the events at the Natanz nuclear facility, could one consider that the applicability of IHL was triggered?
c. If IHL does not apply, which framework regulates the matter? With what consequences?

III. Conduct of hostilities

1. (Document A, paras. 1, 2, 10, 11, 21- 23; Document B, paras. 2, 3, 10, 12, 13)
   a. Is there a difference between a cyber-attack and an attack under IHL? (P I, Art. 49)
   b. (Document A, 1, 2, 10, 11, 21 – 23; Document B, 2, 10, 12, 13) Did the Stuxnet attack comply with the principle of distinction when it was unleashed? (P I, Art. 48, 51, 52)
   c. Were Iran's centrifuges a legitimate military objective? Can an attack against a civilian object be considered lawful if the attack does not result in destruction or if its effects are reversible? (P I, Art. 52)
   d. (Document B, para. 3) Is the prohibition contained in Art. 56 P I dependent on the type of weapons or methods of warfare used? Was the prohibition violated in the present case? If Stuxnet would have unleashed destructive radiological materials, what would likely have been Tehran's reaction? Why?
   e. In general, does the use of Computer Network Attacks (CNA) expand the range of legitimate targets? Why/Why not?
   f. Would uniformed military personnel, computer operators launching viruses or accessing the opponent's network be considered spies under IHL? Legitimate targets? In the present case? (P I, Art. 46, 48, 52)

IV. Proportionality and Precautions

1. (Document, paras. 2, 21 – 24; Document B, para. 13)
   a. What were the incidental effects of the Stuxnet attack? Is the principle of proportionality relevant in the present case? Why/Why not? (P I, Art. 51, 57)
   b. Does the injunction to take precautions in both attack and defence apply during peacetime? Are these questions relevant in the present case? (P I, Art. 57, 58)

V. New Weapons

1. (Document A, paras. 13 – 14)
   a. In your opinion, did the development of the Stuxnet virus comply with Article 36? Is it feasible to apply Article 36 to situations of cyberwarfare?

VI. Miscellaneous

1.
   a. Did the use of Stuxnet violate the UN Charter?
   b. In your opinion, should IHL be adapted to address the realities of the changing cyber landscape and its potential battlefields?

c. From an IHL perspective, do you see some advantages in cyber warfare? Why?
d. Does the destruction of data constitute an attack under IHL? Can an armed conflict start as a result of such destruction?
e. What is the temporal scope of IHL? Do cyberattacks raise some particular issues in this regard?
f. Did this incident involve the commission of war crimes? In general, do you see some particular problems in relation to the belligerent nexus required for the commission of war crimes and cyber warfare?