Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus ad Bellum and Jus in Bello

Carson Marr

Introduction

It's a seemingly average June day at the Natanz uranium enrichment facility in Esfahan, Iran. All the dials and computer-generated data point to standard operation of the near 5,000 centrifuges.[1] But, as with many other days throughout the 2009 season, today is replete with setbacks, errors, and chronic fatigue failures of Iran's struggling cold-war era IR-1 enrichment devices.[2] A new wave of firings commences, and a state of pandemonium envelops the facility. Discord and mistrust run throughout Iran's nuclear ranks, along with fears of intrusion elsewhere in the nation's cyber infrastructure.[3] With so many failures, it's no wonder why the bosses point fingers at anyone who might be behind the destruction of the centrifuges. Unbeknownst to the facility operators, today isn't busi-

1. Centrifuges are large cylindrical devices comprised of smaller tubes that spin at speeds near 1,000 MHz to enrich nuclear isotopes. Each centrifuge is arranged in a series known as cascades, each varying in size but usually comprised of 164 linked centrifuges. Lindsay, 2013, 380.
2. This chronic fatigue, as opposed to catastrophic failure, was specially implemented to create chaos within the Iranian facility, while keeping likelihood of detection to a minimum. A standard catastrophic-failure attack would have been caught and neutralized almost immediately, despite the man-in-the-middle attack described later.
3. Kello, 2013, 23.

ness as usual at the struggling nuclear facility. At this moment, Natanz is the target of a thoroughly planned bilateral cyberattack over three years in the making.[4]

The plans for this unconventional strike hatched amid growing tensions between Middle Eastern Israeli and Palestinian actors at a crucial stage in the long fought cat-and-mouse game to prevent Iran from attaining nuclear armament capabilities. In 2006, under the purview of United States President George W. Bush, Operation Olympic Games began. This covert campaign ushered in a new phase of the struggle to keep Iran at bay without devolving the region into further turmoil. Since 1957, a precarious situation enveloped the U.S. and Iran as the Iranian state sought to acquire nuclear weapons, while the U.S. and its supporters labored to undermine these attempts. In the earliest days of this feud, then-ally Iran signed a civil nuclear agreement as part of the U.S. Atoms for Peace program.[5] Then, in 1968, Iran signed the Non-Proliferation of Nuclear Weapons Treaty (NPT), but, in 1979, with the growth of the Islamic Revolution, U.S.-Iranian relations were severed. Over the subsequent two decades, despite continued input from Chinese, North Korean, and Pakistani experts, U.S. political efforts kept Iranian nuclear development to a minimum. By 2003, however, despite its prior promise to the International Atomic Energy Agency (IAEA), Iran's capabilities had advanced rapidly. When staunch conservative Mahmoud Ahmadinejad succeeded Iranian President Mohammad Khatami in 2005, Bush demanded that the U.N. Security Council impose strict sanctions on the import and export of sensitive nuclear material. By 2006, these sanctions were still in effect, but the enrichment process was also still grinding along, forcing President Bush to pursue alternative measures to keep Iran at bay.

Destroying Iran's development infrastructure could have neutralized their progress. And a standard airstrike might have accomplished this goal, if it weren't for Iran's efforts to disperse their system throughout the country and away from Israeli borders. In addition, the newest facility at Natanz was largely housed in underground bunkers - areas that were difficult to attack at the time. Nonetheless, a strike would have been feasible. In fact, earlier in the year, Israel requested the necessary bunker-busting munitions from the U.S., a request that Bush emphatically rejected. And, as shown by an Israeli attack on a Syrian nuclear enrichment plant during

4. Although some contest use of the term cyberattack, I side with Rid, Liff, and Junio's determination that the Stuxnet malware strain does in fact fit the criteria.
5. NPR, 2018.

Operation Orchard, a kinetic strike was still within reason. However, the potential blowback could have been immense, and a retributive strike by the Iranians against Israel would have proven disastrous. These circumstances, combined with U.S. involvement in two unpopular wars in Iraq and Pakistan, galvanized public opinion against another "unwinnable war."[6] In November 2007, commencing a tactical strike became all but possible. Despite intelligence agencies' knowledge to the contrary, the widely reported U.S. National Intelligence Estimate assessed that Tehran had not restarted its nuclear program after 2003.[7] Regardless, Israel still sought plans to enact a conventional strike. The outlook was dismal, but in its final effort to keep Israel at bay, and Iran behind schedule, the U.S. had another strategy.

Enter Operation Olympic Games: a covert cyber campaign intended to weaponize a strain of malware to counter the progress of Iranian nuclear pursuits. Already two years in the making, the program was fast-tracked by former President Barack Obama after its initial introduction into the wild in mid-2008. This paper aims to address whether or not the Stuxnet worm cyberattack was ethically acceptable. This analysis will apply metrics of Just War Theory (JWT), as popularized by the United Nations Charter and Geneva Conventions and thoroughly explored by Michael Walzer. First, I will utilize the framework of *jus ad bellum* to uncover whether the cyberwar itself was just. More precisely, I apply the legalist paradigm (LP) to assess whether the cause of the war was just. Next, I explore the concept of *jus in bello* to evaluate whether the U.S. fought this cyberwar justly, with special focus on whether the combatants followed the "laws of war." Note that these two elements of JWT are independent; one can fight a just war unjustly and vice versa.

A cyber conflict is described as an offensive cyberattack for political or strategic purposes and encompasses the responses to the attack as well.[8] Though cyberweapons are not overtly violent and thus do not fit the standard definition of interstate conflict, they have the potential to inflict serious harm and to threaten society.[9] Lucas Kello, Director of the Centre

6. This phrase represented the attitude that many had towards the Vietnam War, from the U.S. perspective. For more information, see the following article from the Wilson Center. https://www.wilsoncenter.org/event/vietnam-the-history-unwinnable-war-1945-1975.
7. Raas, 2007, 7-33.
8. Rid, 2012.
9. Kello, 2013, 8.

for Technology and Global Affairs at Oxford University,[10] divides cyberattacks into their direct and indirect consequences, concluding that, by definition, a cyberattack must "produce significant physical destruction or loss of life."[11] In fact, according to Timothy Junio, a former cyberwarfare strategist for the Central Intelligence Agency (CIA) and Office of the Secretary of Defense, non-lethal cyberattacks have the potential to be more expensive and damaging than traditional warfare.[12] An important factor here is the cost and probability of cyber war in relation to other conventional forms of conflict.[13] So, while the 2007 DDoS attacks on Estonia do not qualify as cyberwarfare, the Stuxnet cyberweapon and its usage does.[14] Thus, despite rampant "threat inflation" arguments espoused by skeptics like Thomas Rid, a leading international cybersecurity expert, the cyber threat posed by the Stuxnet worm and other cyberweapons have the potential to qualify as acts of war and, as such, ought to be taken seriously.[15]

Jus ad Bellum

Mark Amstutz separates the concept of *jus ad bellum* into six necessary criteria used for generalizing whether a conflict is just: just cause, competent authority, right intention, limited objectives, last resort, and reasonable hope of success.[16] With just cause criteria, Amstutz indicates that the only legitimate justification for war is to deter aggression, defend against unjust attack, or right a grievous wrong.[17] Focusing on the deterrence prong, we reach our first ethical and definitional dilemma. Deterrence bifurcates into two forms of just and unjust violence—preemptive attacks and preventative attacks. First, preemptive attacks require empirically demonstrable imminent danger. In the case of Stuxnet, only speculation abounds, and this is not enough to meet the stringent requirements for

10. https://www.politics.ox.ac.uk/academic-staff/lucas-kello.html.
11. Ibid, 20.
12. Junio, 2013, 126.
13. Ibid, 127.
14. DDoS, or Distributed Denial of Service, is a method for enlisting "zombie" machines to send bogus requests intended to overwhelm a server to block legitimate traffic from routing appropriately. For a more in-depth report on the Estonian case see Kello, 2013, 24-25.
15. Rid, 2012.
16. Amstutz, 2013, 70.
17. Ibid, 141.

a preemptive attack.[18] This is because JWT seeks to limit the occasions for war, and allowing for a country to enact a preemptive strike to stall a forecasted future attack could open Pandora's box in the realm of international relations. The requisite information needed to enact a preemptive strike is incredibly specific and explicit, and Stuxnet does not meet this burden of proof, thus failing as a preemptive strike.

Prevention, the second angle to deterrence of aggression, is rooted in whether Iran would have soon achieved nuclear supremacy and what Tehran would have done with that capacity. As with all preventative strikes, we cannot know for sure what Iran would have done if given the chance to employ nuclear weapons, but, by 2012, Iran still had not "broken out" of the NPT. Even today, Iran agrees to remove most of its enriched uranium.[19] To echo Amstutz, "must a country wait until a rogue state launches a ballistic missile tipped with a WMD before it can legitimately attack that state?"[20] Here, we are in a unique position to look back on the Stuxnet operation with knowledge of the damage that it posed. Given U.S. and Israeli accounts, this was a preventative strike to ensure that the unstable Iranian government didn't have the capacity to strike at will in the future. Looking at Michael Walzer's criteria for first strikes, we see that "sufficient threat" is necessary. This is satisfied when the following are present: a manifest intent to injure, active preparation that establishes a positive danger, and a situation in which waiting greatly magnifies the risk.[21] But the difficulty here is whether Iran established intent. From the logical perspective, if Iran did not plan to use the enriched uranium for nuclear devices, then Tehran would likely abide by the NPT to avoid further sanctions. On the other hand, Iran may have planned to use the nuclear weapons as a deterrent force against Israel and the U.S. However, this preventative framework usually applies to a manifest intent to injure, further complicating the matter because Israel and the U.S. indicated no intent to use nuclear force. We cannot assume that imminent danger preceded the Stuxnet attack, nor that Iran would have used nuclear weapons if given the chance. As a result, just cause criteria rejects this act of aggression as morally impermissible, because neither preemption nor prevention established a manifest intent to injure.

18. Ibid, 149.
19. CNN, 2018.
20. Amstutz, 2013, 153.
21. Walzer, 2015, 81.

The question of competent authority is often difficult in the cyberspace because of the attribution problem, but, in this scenario, the challenge is somewhat ambiguous. Assuming the U.S. and Israeli governments were behind this attack, and that the attacks were not committed by rogue developers, it is clearly an action authorized by a legitimate government.[22] With conventional acts of warfare, attribution is relatively simple; it is easy to tell whose troops march on your borders or which nation's planes drop bombs, but this type of delineation is far more challenging with Stuxnet. Cyberconflict blurs the lines of attribution, and, in this case, no government has yet claimed the acts of war as their own.[23] This raises the question of whether authorization can be given without appropriate attribution. In the past, we have seen terrorist groups fight unjust wars because they act outside of the sphere of governmental authority. But, never have we seen a government acting authoritatively without attribution of actions as their own. In short, because of today's underlying internet architecture, and despite cutting-edge forensic analysis, it is very difficult to determine who committed a technological action, why they did it, and what the result was.[24] Attribution is critical to deterrence (the concept that one can deter another from acting for fear of reprisal). It is difficult to retaliate against an unidentified enemy.[25] To this end, the authority of an unattributed attack is largely still an open topic in the field of cyberwarfare. I would argue more attention ought to be paid to it lest former Secretary of Defense Leon Panetta's ominous "cyber Pearl Harbor" come to fruition.[26]

Regarding right intention (seeks to restore a just peace), limited objectives (encompasses the obvious, combined with proportionality), last resort (exhaustion of peaceful means), and reasonable hope of success, the case is relatively straightforward. Despite a constant state of unrest

22. John Stone pursues this argument in more detail in his piece, "Cyber War Will Take Place!" and every other article cited in this piece attributes the attack to the United States and Israel.
23. While most of the literature defends the thought that Stuxnet was created for and by the United States and Israel, there are defensible cases made to the contrary. One such case by Jeffrey Carr in Forbes, points the finger at a Finnish-Chinese collaboration. https://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/#30898f062b58.
24. Clark, 2010, 25-30.
25. Ibid.
26. Kushner, 2013, 4.

among nations in the Middle East for many decades, Stuxnet sought to increase the amount of time that the United Nations had to debate various policies and grant Iran an appropriate window to respond to them. So, while a just peace was not present to begin with, this act of war sought to precipitate it more rapidly than conventional arms might, by keeping Iran from obtaining a nuclear football. While delaying Iranian procurement of nuclear capability is somewhat nebulous, this is all that one can afford short of invading the nation or taking even more drastic measures. An unstable regime like Iran tends toward the procurement of nuclear armaments, and thus war can only delay or exacerbate the process. Diplomacy can stem the flow of development, but the UN needed more time to debate and implement austerity measures.[27] Finally, last resort is rather interesting, because this act of war served as a relatively mellow means of pursuing peace without resorting to conventional bloody warfare. While there was potential for reprisal by a conventional Iranian force, this was not likely nor has it ever transpired. By this account, Stuxnet sought to increase the number of peaceful means of diplomatic negotiation before a kinetic strike and aggressive conflict were necessary. Thus, this action had a reasonable hope of success in enabling communicative parties to remain at the negotiating table longer, an unlikely feat had Iran reached nuclear supremacy or Israel authorized preemptive strikes.

Drawing on each of these six essential prongs of the *jus ad bellum* approach to JWT, we have a clear picture painting the U.S.-Israeli cyberwar as morally acceptable on five counts-the one exception being it did not establish just cause. Insofar as Iran would have used its nuclear armaments to harm the Israeli people and throw the rest of the region into turmoil, this cyberweapon could have provided just cause for a competent authority as evidenced by right intention, limited objectives, and a reasonable hope of success. But Iran's intentions were not empirically demonstrable, no matter how conclusive the speculation appears. As a result, this cyber conflict, though an unjust war, still could have been justly fought. As such, we now must look at the specifics of what transpired as it relates to the ethical frameworks of JWT.

27. I assess proportionality more thoroughly in the next section's discussion of jus in bello.

Jus in Bello

We now hone in on discrimination and proportionality in the scope of the unjust cyberwar. Discrimination dictates that a nation may apply military force only against the political leadership and military forces of a state,[28] and the attack must avoid both civilian harm and minimize collateral damage at all costs. To assess whether this was the case, we must look deeper into the inner workings of Stuxnet: a dual warhead comprised of what is known as a "man-in-the-middle" attack[29] and the technical payload of the malware. The latter was a series of system rootkit command and control (C2) calls issued to the Programmable Logic Controllers (PLC), which monitored and managed the complicated centrifuges.[30] Traditional malware travels through networks and the internet, but, in an added level of security, the Natanz nuclear center was contained within an "air-gaped" network. This means that, barring any security mishaps or human error, there is no communication from within the Natanz network to the world surrounding it. This posed a problem for the designers of the malware, so they utilized a "zero-day" exploit in LNK files to provide auto-execution capabilities and transferred them through flash-drives used by unwitting Iranian contractors. Once the malware bridged the air-gap, it continued to spread through the system.

Stuxnet is a malware strain known as a worm because it aggressively replicates itself to spread throughout a network. In the process of doing this, the malware constantly logged information about the network it was exploring and searched for very specific scenarios before it unleashed its full potential. Once the worm worked its way into the desired piece of equipment, it began an indefinite two-month cycle of promoting chronic fatigue in specific models of IR-1 uranium enrichment devices.[31] If the malware hadn't reached its destination, or found a new piece of machin-

28. Amstutz, 2013.
29. These are eerily similar to bank heist scenes in which crooks loop doctored footage on the security guard's screens. Here, the developers of Stuxnet tricked the properly functioning monitoring systems to read standard output regardless of what was really happening within the device.
30. See Junio, 2013, 130 for a more concrete discussion of command and control issues as they arise within the scope of cyber space.
31. Once a SIMATIC device is found and the man-in-the-middle attack is underway, Stuxnet speeds up the IR-1 centrifuge to 1410 MHz (outside of its operating capacity) for 15 minutes. Then, it returns to regular 1064 MHz for 27 days, then down to 2 Hz (too slow to enrich uranium) for 50 minutes, then back to standard 1064 MHz for 27 days, and the process loops.

ery to jump to after two weeks, it terminated immediately. Among other attempts to limit propagation and discriminate its targets, every time the malware ran on a new device, it ensured that the current date was before June 24, 2012, apparently the termination date of the mission.[32]

At some point during the process of propagating through Natanz's air-gaped network, the pernicious code spread onto an unwitting engineer's personal computer. When she took said computer home and connected it to the internet, in a matter of moments, Stuxnet was free. After a short stint in Iran, the malware made its way onto systems in over 150 countries and upwards of 100,000 hosts, including the systems of Chevron Corporation in the U.S.[33] What is incredible about the spread of this malware is that it did nothing to the civilian devices it encountered, save reducing network bandwidth. In a remarkable showing of discriminative execution, this piece of malware, which intended to wreak havoc on enemy infrastructure, was robust enough to restrain itself in an uncontained environment. Double effect mandates that a particular action is morally acceptable given the act is good, the direct effect is morally acceptable, the actor's intention is good, and the good effect is sufficiently good.[34] This restraint on collateral damage proves to be a simple moral calculus for Stuxnet, despite its introduction onto 100,000 civilian devices, because of the adept discrimination practiced by the malware and its human developers.

The Doctrine of Double Effect (DDE) espoused by Walzer, and critiqued by philosopher Henry Sidgwick, requires that the harm done must not be out of proportion to the good achieved. The significant additional condition to this framework is the double intention condition, in which the intent of the actor weighs heavily on the moral standing of the action itself. For example, if one desired to bomb a city with the intent of killing civilians to demoralize an enemy, he is morally abhorrent. If the same person commits the same bombing campaign, but with the intent of killing military targets, knowing that civilians will be killed in the process, he is morally admirable so long as he attempts to reduce the number of civilian deaths.[35] Applying this to Stuxnet, we see a noble attempt to plan for contingencies and protect innocent civilians from the destructive malware that the developers built. In doing so, we can assume that the developers

32. Kello, 16-18.
33. Symantec, 2011, 5.
34. Walzer, 2015, 153-156.
35. Walzer, 2015.

had no intent to hurt civilians and thus upheld DDE and double intention.

Jus in bello provides a framework for assessing the moral standing of a war-time action. In the case of Stuxnet and its clear intent to protect civilians, plan for contingencies, avoid damaging anyone other than the enemy, and sustain proportionality, we see *jus in bello* exemplified. This is a demonstrable success in the realm of DDE and discrimination, and it provides insight into a well-fought cyberwar.

Conclusion

In parsing the evidence laid bare by the divulgence of the Stuxnet cyber-attack and mapping it onto Just War Theory's jus ad bellum and jus in bello, we obtain a full picture of the first cyberweapon ever reported and likely the first case of genuine cyberwarfare in history. I used JWT because it presents the most cohesive tradition of military ethics in use today, and it seeks to limit the occasions for war, perhaps, more than any other moral framework. I make the case that the cyberwar was, in fact, morally praiseworthy in how it kept human lives off the battlefield and worked to effectively discriminate the destruction of enemy systems while avoiding wreaking havoc on civilian systems. But, the war itself was unjust because the aggressor did not prove just cause, in large part because JWT requires the preponderance of material evidence. In assessing the efficacy of this cyberwar, we can be none too wary of the precedent set by endorsing or critiquing it. After all, reprisals may have already happened against the U.S. or Israel for its implied part in the cyberconflict despite the attribution problem. Future research needs to dive deeper into the moral implications of world-wide attack vectors without a standard ability to attribute to the perpetrator and what that means for competent authority in jus ad bellum. Also, we do not know the extent to which cyberwarfare preserves or damages the lives of civilians. I echo prior writers who note that we may fight the next major war in cyberspace. As a result, Stuxnet could be only the mildest weaponized malware variant, equivalent to a musket prior to the advent of the Gatling gun. Thus, despite the concession that Stuxnet was an unjust war fought justly, we ought to tread lightly in how we relate Just War Theory to future cases of cyberwarfare.

References

Albright, David, Paul Brannan, Andrea Stricker, Christina Walrond, and Houson Wood. "Preventing Iran from Getting Nuclear Weapons: Constraining Its Future Nuclear Options." Institute for Science and International Security, 5 March 2012.

Amstutz, Mark R. *International Ethics: Concepts, Theories, and Cases in Global Politics*. Lanham: Rowman & Littlefield, 2013.

Broad, William, John Markoff and David E. Sanger. "Stuxnet Worm Used Against Iran Was Tested in Israel." The New York Times. January 15, 2011. Accessed April 23, 2018.

Carr, Jeffrey. "The New York Times Fails to Deliver Stuxnet's Creators." Forbes. April 11, 2011. Accessed April 23, 2018.

Clark, David D. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, D.C.: National Academies Press, 2010: 25-40.

CNN. "Iran's Nuclear Capabilities Fast Facts." March 30, 2018. Accessed April 23, 2018.

Falliere, Nicolas, Liam Murchu, and Eric Chien. W32.Stuxnet Dossier. Version 1.4 Symantec Security Response. 2011: 1-69.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth | Belfer Center for Science and International Affairs." Harvard Kennedy School Belfer Center for Science and International Affairs. Fall 2013.

Junio, Timothy J. (2013) "How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate." *Journal of Strategic Studies*, 36:1, 125-133.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." The Meaning of the Cyber Revolution: Perils to Theory and Statecraft | Publications | News and Media. October 2013. Accessed April 23, 2018.

Liff, Adam P. (2012) "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyber Warfare Capabilites and Interstate War." *Journal of Strategic Studies*, 35:3, 401-428.

Lindsay, Jon R. (2013) "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, 22:3, 365-404.

NPR. "Timeline: The U.S., Iran And The Nuclear Question." August 25, 2009. Accessed April 23, 2018.

Raas, Whitney, and Austin Long. "Osirak Redux? Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities." *International Security* 31, no. 4 (Spring 2007): 7–33.

Rid, Thomas. (2012) "Cyber War Will Not Take Place." *Journal of Strategic Studies*, 35:1, 5-32.

Stone, John. (2013) "Cyber War Will Take Place!" *Journal of Strategic Studies*, 36:1, 101-108.

Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. 5th ed. New York, NY: Basic Books, 2015.