**Ethical Dimensions of Cyberconflict**

John P. Peck

Department of Cybersecurity, Old Dominion University

PHIL 355E: Cybersecurity Ethics

Prof. Nathaniel Nicol

April 11, 2024

**Ethical Dimensions of Cyberconflict**

The cyberwar between Israel and Iran has manifested through a lot of targeted attacks that interrupt life and critical infrastructure in both nations. This conflict has been going on for over a decade, and intensified during the COVID-19 with cyber operations against citizens' water and sanitation facilities in Israel, and similarly aggressive attacks on Iran’s petrol distribution systems. These attacks have caused significant disruptions shown by the incident reported where Iranian citizens were unable to purchase subsidized fuel due to a cyberattack. This in turn leaves thousands stranded and creates a lot of domestic chaos. Also, the ethical side of these cyber engagements raise serious questions, as both nations continue to engage in a tit-for-tat digital warfare without any formal acknowledgment or declaration of cyberwar.

This cyber conflict not only highlights the strategic use of cyber capabilities to put some pressure and retaliate but it also shows the vulnerabilities inherent within national infrastructures that heavily rely on digital technologies. Each side's defensive and retaliatory actions blur the lines between offense and defense. The complexity of this cyber conflict along with the potential risks to innocent people and the loss of essential services gives us a good case analysis.

In this Case Analysis, I will argue that the Ethics of Care shows us that the cyberwar between Israel and Iran is not just because it perpetuates a cycle of retaliation that prioritizes nationalistic aggression over the well-being and security of individual citizens in both nations. This approach shows the mutual interdependence and care required for societal and international thriving, making the conflict unjust.

***Boylan’s Perspective***

Michael Boylan wrote an article called "Can there be a Just Cyber War?" This article gives us a good idea for understanding the ethical implications of cyber warfare with focus on the transformation of warfare examples due to technological advancements. A main idea in his argument is the distinction between traditional warfare which has well-established rules of engagement, and cyber warfare which operates in a largely unregulated and unclear domain. Boylan questions the existing Just War Theory in the context of cyber conflicts, given their unique characteristics such as the difficulty in attacks and the dual use nature of digital infrastructures that serve both civilian and military purposes.

The cyberwar between Israel and Iran shows these challenges. The attacks on civilian infrastructure such as water facilities and fuel systems blur the lines between military and civilian targets which complicates the ethical assessment of these actions. From Boylan's perspective, the principle of discrimination which is a core idea of Just War Theory that demands a clear distinction between combatants and non-combatants. This is difficult to do in cyber conflicts. This is problematic given that both countries have engaged in actions that seemingly target or result in the disruption of civilian life which violates this principle.

The Ethics of Care emphasizes the importance of maintaining relationships based on mutual interdependence and care for one another. This ethical tool prioritizes the protection and flourishing of relationships over abstract principles of justice or impartiality. In the context of the Israel-Iran cyber conflict, the Ethics of Care would deal with the actions of both nations for failing to prioritize the well being of their own and each other's citizens. Cyber attacks that disrupt essential services not only fail to protect these relationships but harm them.

Furthermore, the Ethics of Care talks about a consideration of how actions affect all people involved. The impact of these cyber attacks on Israelis and Iranians who are the unintended victims of these attacks must be considered in this. The disruption of essential services like water, healthcare, and fuel has significant negative effects on the lives of millions.

The right thing to have done, from an Ethics of Care perspective, would have been for both nations to find different ways to fight that do not involve the targeting of civilian infrastructure or the broad disruption of civilian life. Some ways that could have done it differently can be cyber defense strengthening without offensive attacks, or international mediation to address the root causes of the conflict. This approach not only prevents harm to innocent people but also helps maintain the social part that is important for peace and security.

Also, talking about cyber norms and establishing clear rules and regulations around state behavior in cyberspace could mitigate such conflicts in the future. This relates with the Ethics of Care’s emphasis on fostering relationships and mutual respect to communities and nations, encouraging a team effort rather than an enemy approach to international relationships and cyber security.

In conclusion, analyzing the Israel-Iran cyber conflict through Boylan’s framework and the Ethics of Care shows us the cracks in both the traditional paradigms of Just War Theory and the current retaliatory approaches by the nations. A caring ethical approach would help support strategies that protect and improve the well being of all affected individuals.

***Mariarosaria Taddeo's Perspective***

Mariarosaria Taddeo's article "An Analysis For A Just Cyber Warfare" goes into the complexness and ethical dilemmas introduced by cyber warfare within the Just War Theory and Information Ethics. Taddeo mentions that while Just War Theory provides a foundational ethical assessment of war and it is insufficient on its own to address cyber warfare due to the non physical and often non violent nature of cyber conflicts. This lack of cyber related rules from this theory is because of the focus on physical violence and visible damage, which are less common in cyber operations. Taddeo mentioned merging this theory with information ethics to create a more in depth theory that acknowledges the informational nature of cyber warfare and its potential for widespread,non-physical, harm.

In the context of the Israel-Iran cyberwar, Taddeo's insights help us understand the ethical implications of cyber attacks that disrupt civilian life without causing direct physical harm. These actions challenge traditional notions of warfare as they often involve tactics like disabling national infrastructure which can have huge consequences for civilians without involving direct violence. This raises ethical questions under the Just War Theory principle of discrimination which is about a clear distinction between combatants and non-combatants.

Using the Ethics of Care in this analysis, we recognize the importance of maintaining and nurturing relationships not only within communities but also between nations. This ethical tool emphasizes actions that foster interdependence and mutual respect. In the cyber conflict between Israel and Iran, the repeated breaches against civilian infrastructure which includes attacks on water facilities, fuel systems, and hospitals shows a neglect of care for the well-being of people who rely on these services.

The right way would have been to avoid targeting infrastructure that primarily serves civilians and instead focus on diplomatic parts or target only the military capabilities of the opponent. This would minimize harm to civilians and reflect a caring approach to conflict resolution which considers the welfare of all individuals affected by these actions.

Furthermore, Taddeo’s integration of Information Ethics calls for an assessment of cyber actions based on their effects on the 'Infosphere' which is the total of all informational environments affected by digital actions including those that impact non-physical domains. According to Information Ethics actions that cause informational entropy which is any form of destruction or disruption in the Infosphere are considered unethical. The cyberwar actions by both Israel and Iran which induced huge disruptions in each other’s national infrastructures, can be viewed as increasing entropy in the Infosphere, which goes against the ethical guidelines by Information Ethics.

From an Ethics of Care perspective the right thing to have done would have involved more responsible behavior in the digital realm recognizing the interconnected nature of our world where actions in cyberspace can have real world impacts on millions of people. Both nations could have worked towards establishing norms and agreements that specifically restrict the use of cyber operations against civilian infrastructure. This approach aligns with the principles of caring for the wellbeing of individuals and fostering a responsible and cooperative international community.

In conclusion, when examining the cyberwar between Israel and Iran through the combined parts of Taddeo's ethical framework and the Ethics of Care, it becomes clear that actions taken by both sides failed to adhere to ethical guidelines that prioritize the protection and care of civilians and the stability of the Infosphere. A more caring and ethically sound approach would be team efforts to minimize harm and protect the interconnected digital and physical lives of all people.

***Conclusion***

In this analysis, I have talked about the ethical dimensions of the ongoing cyberwar between Israel and Iran through the lenses of Just War Theory, Information Ethics, and the Ethics of Care. The key argument is that both nations' cyber activities, particularly those targeting civilian infrastructure, do not align with ethical standards that emphasize minimizing harm and respecting non-combatant immunity. The integration of Information Ethics with Just War Theory provides a great analysis for looking at the actions within cyber conflicts which shows the importance of considering informational damage alongside physical violence.

One potential objection to my analysis could be the realm of international security; the ethical considerations may need to be second to strategic and defensive plans. People might argue that the unpredictable and stealthy nature of cyber threats justifies aggressive tactics to ensure national security. While these concerns are valid, prioritizing ethics in cyberwarfare is crucial to prevent cycles of retaliation that could lead to larger instability and harm especially to civilians.

The broader implication of this discussion extends to other states engaged in or vulnerable to cyber conflicts. Establishing international agreements that prioritize ethical considerations in cyber operations could help reduce the risk of harm to civilian life and global security.

While the argument presented prioritizes ethical considerations, it recognizes the complexness of making such norms in the secretive realm of international cyber operations. The challenge lies in aligning national security interests with ethical principles. I hope that we are able to make some framework as the next big war will be in cyberspace.

**References**

Boylan, M. (2013). *Can there be a Just Cyber War?* Journal of Applied Ethics and Philosophy, 5, 11-22.

Taddeo, M. (2012). *An Analysis for a Just Cyber Warfare.*

Middle East Monitor. (2021, November 8). The cyberwar between Israel and Iran is heating up Middle East Monitor. https://www.middleeastmonitor.com/20211108-the-cyberwar-between-israel-and-iran-is-heating-up/

Will there be a cyber war with Iran? (2021, October 27). [Video]. NBC News. https://www.nbcnews.com/news/world/cyberattack-blamed-iran-gas-stations-hit-major-disruptions-rcna3806