Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: CYSE 201S (19044)
Date: 11/17/2024

Article Review 2: "Narrow windows of opportunity: the limited utility of cyber operations in war" by Frederik A H Pedersen, Jeppe T Jacobsen

From Journal of Cybersecurity, Volume 10, Issue 1, 2024, tyae012,
https://doi.org/10.1093/cybsec/tyae014

Introduction

This scholarly article evaluates the use of offensive cyber operations in conventional warfare, through the real-world case study of the ongoing Russo-Ukraine War. The key question the article asks and attempts to answer is "How are offensive cyber operations employed in conventional warfighting, and what is their utility for the warfighting?" (Pedersen, Jacobsen, 2024). The article primarily relies on the TECI model to analyze the performance of offensive cyber operations used to support conventional warfare during the conflict. The TECI model is built specifically to evaluate offensive cyber operations and uses four variables that stand for: Target, Effect, Complexity, and Integration (Pedersen, Jacobsen, 2024). The key takeaway from the authors' assessment of the ongoing war is that there is currently limited utility for offensive operations during war, and list several factors for why they are of limited utility. These factors include the unsuitability of offensive cyber operations to actually achieve physical destruction of a target, the heightened risk of failure, the increased costs and complexity of these operations relative to the desired effects and their success, and the great difficulty of achieving concurrent effects through coordination between conventional warfare and offensive cyber operations (Pedersen, Jacobsen, 2024). However, the authors do identify two instances where offensive operations do have utility to support conventional warfare. According to the authors, one instance is at the very beginning of armed and open conflict between two parties, when there is increased opportunity to coordinate the effects of cyber operations with conventional warfare at the operational and tactical level before the fighting begins (Pedersen, Jacobsen, 2024). The second instance is at the strategic level when targeting the opponents' critical infrastructure, such as their communications networks or energy grid through the use of less complex cyber operations (Pedersen, Jacobsen, 2024).

How the topic relates to the principles of social sciences

As the study notes, cyber operations have always been conducted between nation-state actors, such as between Russia and Ukraine. However, the Russia-Ukraine War is one of the first full-scale armed conflicts between nation-state actors being conducted in the relatively new warfighting domain of cyberspace in addition to the air, land, and sea domains. This article relates directly to how social forces such as politics affect cybersecurity. Nation states develop cybersecurity policies to protect their key strategic interests and means of projecting power, such as their critical infrastructure. Furthermore, the authors note that their is "increasing political acceptance of cyberspace as a domain for military operations, and with more and more states investing in military cyber capabilities" (Pedersen, Jacobsen, 2024. In the modern digital world, nations such as Ukraine must constantly protect their transportation, communications, and energy systems in cyberspace to ensure their population and economy can function properly and prosper. In addition, nation-states must now treat cyberspace as another domain of fighting war. The political leaders must now

take into account not only how they would prosecute a war on land or in the air, but also through computers networks to both protect their own assets but also to attack their opponents assets to achieve their strategic goals. Furthermore, political decisions at the national level, such as going to war, directly affect individual citizens across the entire population. These decisions can affect how people conduct their day to day lives in cyberspace. The desired effect of an offensive cyberattack on the national power grid or internet may be to prevent the opposing government's military from responding to a group invasion through their border. However, this can also have much more wide-ranging effects that deny civilians in the target country the ability to access their financial assets online, their ability to conduct work through the internet, and their ability to contact their families on social media during a crisis.

This article also relates to the sociological paradigm of structural functionalism. The function of a nation's military is to be a stabilizing force that protects society, the government and its citizens from foreign aggression in all domains of conflict. A nation's military forces are typically composed of the army, which fights on land with infantry, tanks, and artillery. Their air force includes fighter planes, stealth bombers, and missiles to fight in the air. The navy uses ships, submarines, and marines to conduct operations on the ocean. Historically, these separate branches would operate independently of each other, with limited coordination. However, as their systems have become more complex and the nature of warfare has become much more integrated through computer networks, a whole new domain in cyberspace has emerged. The military must now contend with how to defend society in cyberspace, as well as develop methods to attack an opponent in cyberspace if needed.

The study's research questions or hypotheses

As previously stated, the key question the article asks and attempts to answer is "How are offensive cyber operations employed in conventional warfighting, and what is their utility for the warfighting?" (Pedersen, Jacobsen, 2024). The authors attempted to answer this question through studying field data derived from the Russia-Ukraine War, starting in February 2022 and ongoing as of November 2024.

Types of research methods used

The authors primarily relied on field data gathered from two sources of empirical data for this article, the CyberPeace Institute (CPI) and Microsoft. the Russia-Ukraine War (Pedersen, Jacobsen, 2024). The timeframe for the field data used in the article covers the period of January through December 2022 and analyzes Russian state actors' cyber-attacks conducted in Ukrainian cyberspace (Pedersen, Jacobsen, 2024).

Types of data and analysis done

The authors primarily relied on two sources of empirical data for this article, the CyberPeace Institute (CPI) and Microsoft, but openly acknowledge the limitations of using these sources since neither are free from bias when reporting on the Russia-Ukraine War (Pedersen, Jacobsen, 2024). The authors are clear in stating that Microsoft has a financial motivation to provide cybersecurity

assistance to the Ukrainian government, and actively aids Ukraine to defend against Russian cyber-attacks (Pedersen, Jacobsen, 2024). The authors also explain that CPI provides cybersecurity services to non-governmental organizations (NGOs) in Ukraine and has an ideological motivation to support Ukraine against Russia's invasion (Pedersen, Jacobsen, 2024). To avoid this bias, the authors claimed they relied solely on "fact-based descriptions and technical analyses" provided by CPI and Microsoft on cyber-attacks conducted against Ukraine by Russia (Pedersen, Jacobsen, 2024). The timeframe for the data used in the article covers the period of January through December 2022 and analyzes Russian state actors' cyber-attacks conducted in Ukrainian cyberspace (Pedersen, Jacobsen, 2024). The authors compared both sources as a control for accuracy and identified commonalities between the two to find trends (Pedersen, Jacobsen, 2024). Finally, the authors acknowledged that there is likely additional technical information on Russian cyber operations that they were not able to access due to the scope and scale of the war, and that their analysis would very likely be enhanced in the future with more data (Pedersen, Jacobsen, 2024).

The authors then developed a model to measure the effectiveness of offensive cyber operations: the TECI model.

Summary of the TECI Model.

Variable	**Definition of Variable**	**Possible Values**	**Definition of Possible Values**
Target	Type of entity whose systems are targeted by the cyber operation	Critical infrastructure Government Media Other targets	Entities in transportation, energy, utilities, and ICT sectors Public authorities, incl. military Entities in mass communication All other types
Effect	Type of direct effects on systems experienced by targets	High effect Medium effect Low effect No effects	Physical destruction Destruction of data Disruption or exfiltration of data Absence of effects
Complexity	Sophistication and scale of the cyber operation	High complexity Medium complexity Low complexity	Novel malware, tools, and techniques Known, possibly modified, malware, tools, and techniques DDoS attacks, simple brute-forcing
Integration	Degree of coordination between cyber and noncyber	High integration Medium integration Low integration No integration	Coordinated in planning and execution Coordinated in

Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: CYSE 201S (19044)
Date: 11/17/2024

	capabilities during the operation		planning Coordinated in general objective Absence of coordination
Reference: Pedersen, Jacobsen, 2024			

How does the topic relate to the challenges, concerns and contributions of marginalized groups

When a nation goes to war, this will directly affect individual citizens across the entire population. These decisions can affect how people conduct their day-to-day lives in cyberspace. If the invading nation decides to conduct an offensive cyberattack on their target's national power grid or internet, the desired effect may be to prevent the opposing government's military from responding to a group invasion through their border. However, this can also have much more wide-ranging effects that deny civilians in the target country the ability to access their financial assets online, their ability to conduct work through the internet, and their ability to contact their families on social media during a crisis. In addition, the invading country could use information operations in cyberspace to influence the target nation's population. The people of Ukraine have had to endure over 10 years of information operations conducted by Russia to divide, manipulate, and discourage them from believing their resistance to Russia is a just or worthy cause.

Conclusion

In their abstract, the authors claim there is limited utility for offensive cyber operations in an ongoing war, but do identify two instances where there is still usefulness. Per the article, the first instance applies at the strategic level: "Cumulative strategic utility is achievable by targeting critical infrastructure and governments in a persistent barrage of less complex cyber operations." (Pedersen, Jacobsen, 2024) The second instance applies at the very start of a shooting conflict at the operational and tactical level, when a nation's armed forces still have the time and capability to integrate cyber operations with other military operations: "Operational and tactical utility is achievable in the beginning of warfighting where the temporal dichotomy is less pronounced because cross-domain integration can be planned before warfighting commences." (Pedersen, Jacobsen, 2024) The study is very limited in its scope and sample, since it's relying on data from the Russia-Ukraine War, a war that is still ongoing. This study shows that there is still a lot of work needed to be done to understand how the offensive cyber operations used in war can affect the local populace and the social constructs of both the attacking and defending countries. The affects of cyber war on a nation can be wide reaching and affect all levels of a society beyond the nation's government, military forces, and economy. Their critical infrastructure, transportation, communication, and energy sectors are also directly affects, and these can have an outsized impact on the civilians and local populace in the region.

Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: CYSE 201S (19044)
Date: 11/17/2024

References

Pedersen, F. A. H., & Jacobsen, J. T. (2024, August 5). *Narrow windows of opportunity: The limited utility of cyber operations in war*. OUP Academic - Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/10/1/tyae014/7727352