Political Implications of the Advancement and Impact of Cyber Warfare on Civilians

Introduction

The advancement of cyber warfare has created an endless amount of new possibilities and scenarios to be prepared for, and it is a problem that may possibly never be solved. Political policies will not be able to address every single concern out there regarding cyber warfare, and even existing issues we have been seeing for decades are still unable to be properly tackled due to how abstract certain matters may be. Because of the nature of cyber warfare as well, nearly every decision made to change national policy regarding cyber defense or offense impacts civilians.

Aside from this, it is common knowledge that harming or endangering civilians is a massive taboo in the global community due to the Geneva Convention. Cyber attacks that are deliberately harming civilians in absurd amounts are a great factor behind how policymakers may change policies regarding foreign troublesome states and how they may be treated politically. Examples may include travel bans, economic sanctions, and denouncement. Travel bans affect civilian tourism, and economic sanctions along with denouncement may harm a country's economy, leading to economic crashes with mass civilian unemployment, starvation, or unavailability of certain services.

Cyber Warfare in Policy and Problems Concerning It

As stated before, cyber warfare addresses an absurd amount of potential scenarios, and even then, it is often not enough. Colarik and Janczewski (2015) bring up key questions regarding cyber policy, with those being what activities must be taken in the case of a cyber attack against

a nuclear power plant, what are appropriate and measured responses to these attacks, and at what level of attack constitutes an act of war. These are many of the abstract concepts that are daunting issues for policymakers, and it is understandable how they are extremely difficult to be solved. Infrastructure is a common target for cyber attacks due to them being able to cause widespread damage against the entire country, including civilians. This, of course, also directly harms civilians as well. Nuclear power plant damage leaves not just the government but innocent civilians out of power and may be life threatening for those who may rely on technology in order to survive. Hospitals not receiving power makes caring for patients much more difficult, forcing them to rely on backup generators. Every piece of damage on infrastructure directly affects civilians, and it is just a matter of "how much is too much" when it comes to policy making. A large morality issue comes from the idea of effective attacks, but at the cost of ultimately doing more harm than good for the rest of the world.

Similar to the idea of "how much is too much," the amount of cyber attacks and severity of them onto a country before being enough to trigger a direct declaration of war is a major area of concern for policy makers. Even "trolling" and the spread of misinformation on internet forums has incited massive outrage amongst politicians, to the point where laws have been passed in certain countries regarding fake news and health disinformation (Mills & Sivelä, 2021). Harder cyber crimes such as sabotage, infrastructure attacks, and espionage are harder to gauge whether they are deserving of a formal war declaration. For example, cyber espionage is a difficult field to navigate, with American senator Marco Rubio saying that "America must retaliate, and not just with sanctions" in response to a Russian hack of American government agencies in 2020. However, a Department of Defense law of war manual specifies physical damage, with examples

being a nuclear plant meltdown or airplane crashes as a result of disabled air traffic control services. This level of confusion and inconsistency regarding laws around cyber policy leaves civilians confused and divided, and may potentially result in civilian deaths, injuries, or other inconveniences while the cyber attacks are not deemed enough as an act of war to officially retaliate against. On the other hand, declaring more cyber attacks an act of war may bring a country and its civilians into a difficult economic or social state as a result of said war.

Conclusion

Civilians are a great concern when it comes to cyber policy, especially with 98% of all U.S. government communications traveling over civilian owned and operated networks as of 2009 (Jensen, 2009), along with civilian providers being the main providers for government software and hardware. Because of this, any damage to civilian infrastructure is essentially damage against government operations as well, and policymakers are well aware of that. Constant care and adjustments are proposed in order to keep civilians safe from cyber attacks, but much of the debate regarding that stems from what the correct decision is to actually achieve that.

Policy makers and politicians attempt to keep the government and people in mind when it comes to cyber warfare, and cyber attacks are planned to try to avoid civilians as collateral damage. However, whether that actually holds true is also a large area of debate and serves for social ramifications for said politicians and policy makers. Civilians being hurt or endangered is a large problem and are major factors when it also comes to the levels of retaliation against cyber attacks.

References

Colarik, A., & Janczewski, L. (2015). Establishing cyber warfare doctrine. Current and Emerging Trends in Cyber Operations, 37–50. https://doi.org/10.1057/9781137455550_3

Jensen, E. T. (2009). Cyber Warfare and Precautions against the Effects of Attacks. https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1224&context=faculty_scholarship

Mills, M. C., & Sivelä, J. (2021). Should spreading anti-vaccine misinformation be criminalised? BMJ. https://doi.org/10.1136/bmj.n272

Wolfe, J., & Pierson, B. (2020, December 19). Explainer-U.S. government hack: Espionage or act of war? Reuters. Retrieved November 6, 2022, from https://www.reuters.com/article/global-cyber-legal/explainer-u-s-government-hack-espionage-or-act-of-war-idUSKBN28T0HH