FOREIGN AFFAIRS
Published by the Council on Foreign Relations

Wednesday, May 13, 2015
The Coming Cyberpeace
Brandon Valeriano and Ryan C. Maness

BRANDON VALERIANO is a Senior Lecturer in Social and Political Sciences at the University of Glasgow. RYAN C. MANESS is a Visiting Fellow of Security and Resilience Studies at Northeastern University in Boston. They are the authors of Cyber War versus Cyber Realities [1]*(Oxford University Press, 2015).*

The Normative Argument Against Cyberwarfare

The era of cyberconflict is upon us; at least, experts seem to accept that cyberattacks are the new normal. In fact, however, evidence suggests that cyberconflict is not as prevalent as many believe. Likewise, the severity of individual cyber events is not increasing, even if the frequency of overall attacks has risen. And an emerging norm against the use of severe state-based cybertactics contradicts fear-mongering news reports about a coming cyberapocalypse. The few isolated incidents of successful state-based cyberattacks do not a trend make. Rather, what we are seeing is cyberespionage and probes, not cyberwarfare. Meanwhile, the international consensus has stabilized around a number of limited acceptable uses of cybertechnology—one that prohibits any dangerous use of force.

Despite fears of a boom in cyberwarfare, there have been no major or dangerous hacks between countries. The closest any states have come to such events occurred when Russia attacked Georgian news outlets and websites in 2008; when Russian forces shut down banking, government, and news websites in Estonia in 2007; when Iran attacked the Saudi Arabian oil firm Saudi Aramco with the Shamoon virus in 2012; and when the United States attempted to sabotage Iran's nuclear power systems from 2007 to 2011 through the Stuxnet worm. The attack on Sony from North Korea is just the latest overhyped cyberattack to date, as the corporate giant has recovered its lost revenues from the attack and its networks are arguably more resilient as a result. Even these are more probes into vulnerabilities than full attacks. Russia's aggressions show that Moscow is willing to use cyberwarfare for disruption and propaganda, but not to inflict injuries or lasting infrastructural damage. The Shamoon incident allowed Iran to punish Saudi Arabia for its alliance with the United States as Tehran faced increased sanctions; the attack destroyed files on Saudi Aramco's computer network but failed to do any lasting damage. The Stuxnet incident also failed to create any lasting damage, as Tehran put more centrifuges online to compensate for virus-based losses and strengthened holes in their system. Further, these supposedly successful cases of cyberattacks are balanced by many more examples of unsuccessful ones. If the future of cyberconflict looks like today, the international community must reassess the severity of the threat.

Cyberattacks have demonstrated themselves to be more smoke than fire. This is not to suggest that incidents are on the decline, however. Distributed denial-of-service attacks and infiltrations increase by the minute—every major organization is probed constantly, but only for weaknesses or new infiltration methods for potential use in the future. Probes and pokes do not destabilize states or change trends within international politics. Even common cyber actions have little effect on levels of cooperation and conflict between states.

NORMCORE IS HERE TO STAY

A protocol of restraint has emerged as the volume of cyberattacks has increased. State-based cyberattacks are expected, and in some cases tolerated, as long as they do not rise to the level of total offensive operations—direct and malicious incidents that could destroy infrastructure or critical facilities. These options are apparently off the table for states, since they would lead to physical confrontation, collateral damage, and economic retaliation.

The reproducibility of cyberattacks has also led states to exercise restraint. Enemies can replicate successful cyberweapons easily if source code and programs find their way into the wild or are reverse-engineered. Cyberweapons are not simple to design, either, which makes their use limited: Stuxnet took years of work by U.S. intelligence (with help from Israel) and cost hundreds of millions of dollars—and it still failed. The risk of creating collateral damage is high, since cyberweaponry cannot provide surgical precision and can spread into other networks of possible allies of the attackers. For example, the Stuxnet worm, intended for Iran’s nuclear program’s network, showed up in Azerbaijan, India, Indonesia, and Pakistan, among other countries. As witnessed in the Russian attack on Georgia, the potential for conflict diffusion is high, as third-party allies can enter conflicts easily. Estonia sent its Computer Emergency Readiness Team experts to Georgia to keep the country’s crucial networks up and running. Poland freed up bandwidth for servers in its territory to keep Georgian government websites up and its people informed. Finally, the risk of retaliation is high, as it is in any war, especially as attribution of perpetrators is getting easier to trace with better forensic techniques. The only drawback is that exposing attribution capabilities often exposes ongoing infiltration methods.

All of these considerations have meant that, so far, cyberconflict has adhered to existing international conflict norms. That there have been no major operations resulting in death or the destruction of physical equipment (outside of the Saudi Aramco incident and Stuxnet) suggests trends toward stability and safety. Cyberoperations are increasing, but only in terms of small-scale actions that have limited utility or damage potential. The truly dangerous cyberactions that many warn against have not occurred, even in situations where observers would think them most likely: within the Ukrainian conflict or during NATO’s 2011 operations in Libya. The only demonstrable cyberactivity in the Ukraine crisis has been espionage-level attacks. There is no propaganda, denial of service, or worm or virus activity, as there was in past conflicts involving Russia and post-Soviet states.

The overall trend in cyberwarfare indicates that the international community is enjoying a period of stability. The chart below demonstrates that although cybertactics are increasingly popular, the severity of these attacks remains low. On a scale of one to five, where one is a nuisance attack (a website being defaced, for example) and five is a cyber-related death, few attacks register above a two.

DRAWING COMPARISONS

Although the public may fear cyberthreats, it remains extremely trusting of the existing digital infrastructure. People trust the Internet with their connections, private contacts, banking information, personal lives, professional careers, and even romantic interests. Such confidence may be unwarranted, but resilience, not apprehension, is key to surviving in the coming era of low-level Internet-based attacks and probes.

States must be willing to make dramatic changes to their perceptions of Internet security and governance if they are to prevent cyberattacks. Most states lack functional cooperation between government and private industry for low-level cyber infiltrations, including the United States and EU countries. In addition to greater cooperation between public and private sectors, states and companies must pursue stronger cyberhygiene regimens (providing internal training to prevent potential threats) and reform the infrastructure that supports banking, electric, and health-care systems. Finally, education initiatives would help empower citizens to understand how the Web handles their transactions. Few understand how online banking, health-care databases, and utility grids work on the Internet. Education can help people—and citizens—understand the true nature of cyberthreats.

Here, we can look to the U.S. experience with terrorism: in both instances, fear is the result of imagined consequences. Terrorism has given birth to an industry built to combat threats, and a similar process is now under way with regard to cyberattacks. The general response to terrorism has been counterproductive and damaging, lending itself to hyperbole and overreaction. It is troubling to see the same path repeated with cyberwarfare, as an industry has sprung up within the private sector and military to meet the threat. The fact that there is little evidence of severe cyberattacks should give pause.

The use of cybertechnology will, of course, continue to spread within all aspects of daily life and international affairs, but the risk of true disruption through cyberwarfare is overblown. We must all shift our cultural understanding of how best to handle cyber issues cooperatively in order to reinforce the newly emerging norm against widespread, damaging use. The world needs institutions to enforce these norms, yet few governing bodies seem willing to undertake this massive effort. China, Russia, and the United Nations, among other actors, have proposed potential frameworks with little success. There is not enough trust in the United States to lead these efforts, given its heavy use of cyberattacks to infiltrate enemy networks. Therefore, the international community collectively must take the lead, because both the West and states such as Russia and China have used cyber actions maliciously.

The Internet will be a theater for future conflict, but this does not mean it will become a critical method of conflict. Like other technologies, cybertactics will support and enhance further methods of violence, rather than becoming the primary focus of military conduct. The Internet remains a sacred place for many; upholding a cybersafety norm will enable the world to maintain a shared digital future.

Source URL: https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace

Links
[1] https://global.oup.com/academic/product/cyber-war-versus-cyber-realities-9780190204792?cc=gb&amp;lang=en&amp;