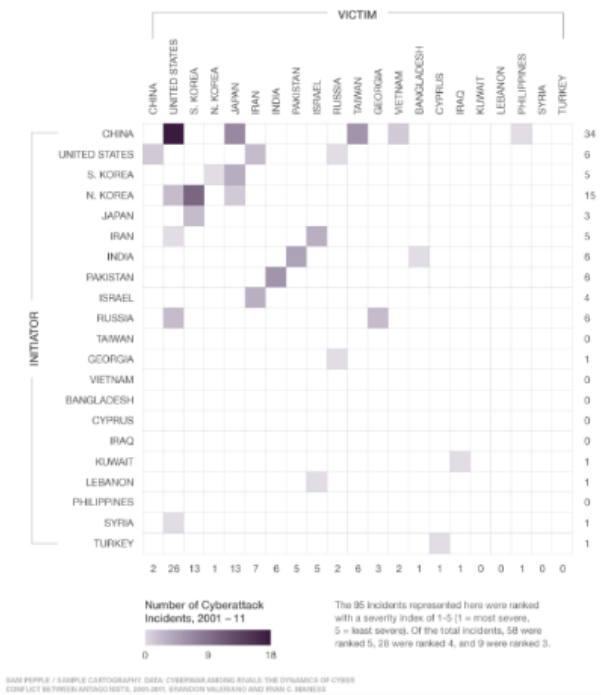
The Fog of Cyberwar

Why the Threat Doesn't Live Up to the Hype

Brandon Valeriano and Ryan Maness

December 6, 2012

Article Summary and Author Biography



A chart showing cybertattacks by initiator and victim between 2001-11. (Sam Pepple / Sample Cartography) **Click here to enlarge.**

In mid-2010, thousands of centrifuges, enriching uranium at Iranian nuclear research facilities, spun out of control. The instruments were mysteriously reprogrammed to operate faster than normal, pushing them to the breaking point. Iranian computer systems, however, inexplicably reported that the centrifuges were operating normally. This incident, it was later revealed, was the work of the infamous Stuxnet computer worm, presumed to be the creation of the United States and Israel, and one of the most sophisticated cyberweapons to date. The infiltration was initially thought to have set back Iran's suspected nuclear weapons program three to five years, although current estimates are in the range of two years to a few months.

Stuxnet was followed by the Flame virus: a new form of malware that infiltrated several networks in Iran and across the Middle East earlier this year. Flame copied text, recorded audio, and deleted files on the computers into which it hacked. Israel and the United States are again the suspected culprits but deny responsibility.

These two attacks generated substantial buzz in the media and among policymakers around the world. Their dramatic nature led some experts to argue that cyberwarfare will fundamentally change the future of international relations, forcing states to rethink their foreign policy. In a speech to the New York business community on October 11, 2012, U.S. Defense Secretary Leon Panetta expressed fear that a cyber version of Pearl Harbor might take the United States by surprise in the near future. He warned that the U.S. government, in addition to national power grids, transportation systems, and financial markets,

are all at risk and that cyberdefense should be at the top of the list of priorities for President Barack Obama's second term.

The Stuxnet and Flame attacks, however, are not the danger signs that some have made them out to be. First of all, the viruses needed to be physically injected into Iranian networks, likely by U.S. or Israeli operatives, suggesting that the tactic still requires traditional intelligence and military operation methods. Second, Stuxnet derailed Iran's nuclear program for only a short period, if at all. And Flame did nothing to slow Iran's nuclear progression directly, because it seems to have been only a data-collection operation.

Some cyberattacks over the past decade have briefly affected state strategic plans, but none has resulted in death or lasting damage. For example, the 2007 cyberattacks on Estonia by Russia shut down networks and government websites and disrupted commerce for a few days, but things swiftly went back to normal. The majority of cyberattacks worldwide have been minor: easily corrected annoyances such as website defacements or basic data theft -- basically the least a state can do when challenged diplomatically.

Our research shows that although warnings about cyberwarfare have become more severe, the actual magnitude and pace of attacks do not match popular perception. Only 20 of 124 active rivals -- defined as the most conflict-prone pairs of states in the system -- engaged in cyberconflict between 2001 and 2011. And there were only 95 total cyberattacks among these 20 rivals. The number of observed attacks pales in comparison to other ongoing threats: a state is 600 times more likely to be the target of a terrorist attack than a cyberattack. We used a severity score ranging from five, which is minimal damage, to one, where death occurs as a direct result from cyberwarfare. Of all 95 cyberattacks in our analysis, the highest score -- that of Stuxnet and Flame -- was only a three.

To be sure, states should defend themselves against cyberwarfare, but throwing vast amounts of money toward a low-level threat does not make sense. The Pentagon estimates it spent $2.6 to $3.2 billion on cybersecurity in fiscal year 2012. And it is likely that such spending will only increase. The U.S. Air Force alone anticipates spending $4.6 billion on cybersecurity in the next year. Even if the looming "fiscal cliff" guts the Defense Department's budget, Panetta has made clear that cybersecurity will remain a top funding priority. At a New York conference on October 12, 2012, he described the United States as being in a "pre-9/11 moment" with regards to cyberwarfare and said that the "attackers are plotting," in reference to the growing capabilities of Russia, China, and Iran.

Of the 20 ongoing interstate rivals in our study, China and the United States cybertargeted each other the most. According to our study, Beijing attacked U.S. assets 18 times and Washington returned fire twice. Two notable attacks were the 2011 Pentagon raid, which stole sensitive files from the Defense Department, and the 2001 theft of Lockheed Martin's F-35 fighter-jet schematics. These attacks get only a moderate severity score because they targeted specific, nonessential state documents and were not intended to affect the general public. Over the same time span, India and Pakistan targeted each other 11 times (India five times, Pakistan six), as did North and South Korea, with North Korea being the aggressor ten times and how many for South Korea launching one return attack. These ranged from minor incidents, such as Pakistan defacing an Indian government website, to more serious ones, such as North Korea stealing sensitive state documents from South Korea.

Israeli-Iranian tensions have risen in recent months, but despite all the talk, this conflict is not playing out in the cybersphere. There were only eight cyberattacks between these states from 2001 to 2011, four launched by Israel, four by Iran. Although Stuxnet and Flame were more severe, Iranian attempts to disrupt government websites have not been very sophisticated. And Israel's near-insistence of an armed conventional attack proves that even the most sophisticated cyberattacks are not changing state behavior.

Cyberattacks are rare, and when they do occur, states are cautious in their use of force. As with conventional and nuclear conflict, some of the principles of deterrence and mutually assured destruction apply. Any aggressor in cyberspace faces the acute threat of blowback: having techniques replicated and repeated against the initiator. Once developed, a cyberweapon can easily be copied and used by a tech-savvy operative with access to a critical system such as the Defense Department's network, which foreign-government hackers have had success infiltrating.

Far from making interstate cyberwarfare more common, the ease of launching an attack actually keeps the tactic in check. Most countries' cyberdefenses are weak, and a state trying to exploit an adversary's weakness may be similarly vulnerable, inviting easy retaliation. An unspoken but powerful international norm against civilian targets further limits the terms of cyberwarfare.

The United States and other responsible powers should restrain their use of the tactic in order to avoid escalation. Attacks such as Flame and Stuxnet are dangerous because they break down the standard of mutually beneficial restraint. These attacks caused little damage in the end, but they still may have encouraged other states to bulk up their own capabilities. The main danger is that one state will overuse the tactic and push other states to do the same.

There is also concern that some countries will overreact to the cyberthreat by clamping down on the freedoms that make the Internet an open and dynamic space. A paranoid government might be tempted to develop extreme defenses, such as a kill switch, that would allow it to shut down all incoming and outgoing cybertraffic. Such a drastic step would have a chilling effect on society, creating more problems than it would solve. This is yet another reason why international standards and communication are crucial.

Cooperation on the cyberwar threat originated in an unlikely place: Estonia. A tiny country with a population of just over one million, it has become a global leader in promoting cyberspace rules and norms that keep states, democratic and autocratic alike, in line. Estonia was thrust into the spotlight after the 2007 cyberattack by and subsequent widespread international condemnation of Russia. Instead of lashing out against its attacker, the small state sought a world forum to discuss its case; since then, it has hosted the International Conference on Cyber Conflict four times. This conference is an outcropping of NATO and hosts countries such as the United States, Canada, the United Kingdom, France, Germany, and Italy.

The gatherings have successfully promoted the adoption of norms and modes of restrained behavior in cyberspace. Developments include the agreement that territorial sovereignty applies to a state's cyberspace, and that cyberwarfare is covered by Article 51 of the UN Charter, which allows a state to take action in response to an attack. Along these same lines, cyberattacks are now being categorized on an intensity scale to help determine what a proper international response might be.

To be sure, cyberterrorism is still a danger. This is a development that will be more difficult to deter. However, fear of a lone cyberterrorist -- like the recent Bond villain in *Skyfall* who is capable of bringing a government to its knees -- is unfounded. To be effective, cyberwarfare requires substantial infrastructure, money, and ground operatives. Because these resources are hard to come by, most cyberattacks launched by rogue individuals are trivial or personal. For example, in 2011 the hacker group Anonymous attacked and shut down the PlayStation network in response to a lawsuit against programmers who modified the software. The network was down for weeks, but aside from creating some disgruntled gamers, the attack left no real damage.

In short, this seldom-used tactic will not change foreign policy calculations anytime soon. Cyberwarfare poses a threat only if it is grossly overused or mismanaged, or if it diverts resources toward a mythical fear and away from real threats.

View This Article as Multiple Pages

Related

ESSAY, MAR/APR 2012

Clear and Present Safety

Micah Zenko and Michael A. Cohen

U.S. officials and national security experts chronically exaggerate foreign threats, suggesting that the world is scarier and more dangerous than ever. But that is just not true. From the U.S. perspective, at least, the world today is remarkably secure, and Washington needs a foreign policy that reflects that reality. Read

ESSAY, JAN 1967

Planning Our Military Forces

Harold Brown

Uncertainty is necessarily the lot of the planner, since the deals with the future. Uncertainty can never be completely removed. However, it can be compensated for, and to do so is a continuing responsibility of those who plan military forces. Primarily this can be done by insuring, in so far as we can, that future weapons and forces will be adaptable to the right range of defense needs or, as defense planners often put it, by insuring flexibility. Read

SNAPSHOT, APRIL 4, 2012

Hacks of Valor

Yochai Benkler

The U.S. government has begun to think of Anonymous, the online network phenomenon, as a threat to national security. This is the wrong approach. Seeing Anonymous primarily as a cybersecurity threat is like analyzing the breadth of the Vietnam antiwar movement and 1960s counterculture by focusing only on the Weathermen. Read