CYBERSPACE AS BATTLESPACE

Black Hat webcast, Oct 9, 2014

Kenneth Geers
2501

Introduction: mission creep

The Internet is still a baby. But the cyberspace around it – the effective connection between computers, computer networks, and humans – is already Planet Earth's greatest technological achievement. Every aspect of human life is different: government, economy, society, and national security.

And this revolution is far from over. The current rate of technological innovation is so quick that no one – not even the National Security Agency – can keep up. Therefore, we must occasionally step back and consider whether the path we are on is an optimal path, or whether certain adjustments should (or even could) be made before it is too late.

There are many Internet-related problems to solve, but this essay is about the military invasion of cyberspace, and attempts to occupy strategic Internet terrain before the next war.

The ramifications are numerous:

1. Hostile activities are taking place in peacetime.
2. Human rights may be needlessly harmed.
3. This dynamic may lead to eternal chaos on the Internet.

The Golden Age of Espionage

First, let's compare cyber war with cyber espionage.

Cyber espionage has existed for more than a generation. Foreign intelligence services leverage the ubiquity, vulnerability, and interconnectivity of computers – and they are getting better at

it every day. The best book on this topic remains *The Cuckoo's Egg,* in which Cliff Stoll, a system administrator at the Lawrence Berkeley National Laboratory in California, traced a $0.75 accounting error all the way back to a German hacker working for the Soviet KGB.

Cyber espionage will be difficult to stop because foreign intelligence is targeted, classified, and (unfortunately) the most popular reading among senior government officials. At a technical level, cyber espionage is often undertaken by well-trained, state-sponsored hackers, which means they are hard to catch, and even harder to prosecute.

And within any given country, if what you are more worried about is the "Surveillance State", I think it is true that law enforcement and counterintelligence will often overstep their bounds. Cops (like everyone else) are overwhelmed by changes in technology, and swimming in a sea of perplexing information. Law enforcement and counterintelligence are getting better at using information technology, but their current position vis-à-vis foreign intelligence hackers is today closer to the script of "No Country for Old Men" – they are usually outgunned.

Evolution not revolution

However, stealing information via computer networks was primarily a natural evolution of espionage. In the collection of foreign intelligence, there are few real constraints. Spy tradecraft includes concealed electronic devices, impersonation, front organizations, false flag operations, murder, and sex.

Every one of these activities has its cyber analog – with the possible exception of murder, but foreign intelligence will eventually perfect that method as well.

Espionage is a game of deception and theft. If and when technology – including computer hacking – can help a spy to accomplish his or her mission, there are few inhibitions. A credible virtual front company is hard to create from scratch, but is faster and cheaper to build than the brick and mortar version.

One final note on cyber espionage: some prominent examples, including Moonlight Maze, the theft of nuclear weapons data, the

loss of the F-35 blueprints, and many more, rise above the level of tactical loss – they are strategic data sets, and strategic national losses.

Espionage vs. attack

There is a crucial difference between cyber espionage (stealing information) and cyber warfare (altering data or data flows in support of a military mission). The former is (relatively) passive, while the latter is aggressive.

In the future, cyber attacks may be defined only by the limits of the attacker's imagination. But for now, let's divide cyber warfare into two primary types:

1. Denial-of-service (DoS)
2. Data modification

DoS is easily understood: either via traditional (e.g. bombs) or digital means, the attacker prevents a legitimate user or computer from accessing a targeted machine or network resource.

Data modification is more ambitious. The attacker aims for nothing short of altering "reality" – at least for a certain period of time. Bombs may appear to be falling when they are not – and vice versa.

If successful, cyber warfare can be both a technical wonder (i.e. a demonstration of elite hacker skills) and a philosophical wonder (i.e. the victim now has a false understanding of reality).

Cyber war: strategy and tactics

Cyber war is no different from any other kind of war. When the violence begins, it means that political and military leaders have decided to use force in an attempt to solve a national security problem. At that point, the goal is to win the conflict – all other considerations are secondary.

There will be an attempt to keep the attack parameters within the "Laws of War", but that is easier said than done – just look at the pictures of Japanese and German cities after World War II.

USAF Gen. Curtis LeMay, mastermind of the Tokyo fire bombing, and post-war Commander of U.S. Strategic Command, said: “I suppose if I had lost the war, I would have been tried as a war criminal … all war is immoral and if you let that bother you, you're not a good soldier.”

The use of digital weapons has many attractive features, including worldwide reach, lightening speed, extreme asymmetry, and potential anonymity. A computer hack is a versatile tool, and can be used to support any traditional war aim – the dissemination of propaganda, the interruption of logistics, the neutralization of weapons systems, and the destruction of critical infrastructure. Every one of us, from a rocket launcher to a cyber war skeptic, needs a reliable computer to properly perform our job.

The success of any given cyber operation may come down to timing and novelty. In certain scenarios, as soon as the war begins, the access points created for cyber espionage can be leveraged to support cyber war.

In the future, it is impossible to say how powerful a cyber attack might be, and a cyber-only war could happen. The simple reason is that everything – including weapons, logistics, and command and control – is now dependent on computers and networks that are vulnerable to hostile takeover.

If there is a future war between major world powers, it is possible that the scale and novelty of the cyber operations could bring down the Internet entirely – perhaps even beyond the duration of the conflict.

Generally speaking, however, hacker tools and tactics play just one part of a larger, more complex conflict – similar to electronic warfare. This is normal; for example, the infantry only constitute about 15% of U.S. Army personnel. There are many ancillary jobs within any military that support its ultimate goal of “killing people” and “breaking things”.

Remember that nation-states will mix and match cyber and non-cyber tools and tactics. There can be cyber vs. cyber operations, cyber vs. non-cyber, and non-cyber vs. cyber.

For a quick review of what the world’s cyber commands are currently saying about their own missions, please see this 2501 blog: “World Cyber Commands: in their own words”.

Nation-state hacking

The difference between nation-state hackers – aka the “Advanced Persistent Threat” – and everyone else is money. Governments do not employ the smartest people, but they can afford an organizational, mission-focused, team-oriented approach to hacking, that includes intelligence officers, linguists, engineers, and more. Such teams enjoy good training, vacations, and retirement plans. If an employee is sick or takes a new job, another person will take his or her seat.

By comparison, cyber defense is an immature discipline; investigations are painstaking and typically inconclusive. Investigators normally have only a few clues to go on, which are insufficient to understand the strategic scope, capabilities, and intentions of the attacker. By the time many intrusions are discovered, the hackers have long since moved on to other targets. And due to jurisdictional boundaries and the “attribution problem”, many attackers operate from an effective safe haven.

In short, against even a good network security team on defense, this is not a fair fight.

Strategic cyber defense

Every nation has a layered defense.

First, every organization has its own network security personnel. However, no matter how intelligent and capable they are, it will be tough to resist a targeted attack by a foreign military.

Second, there is law enforcement, with guns and badges, and the authority to arrest and prosecute. But cyberspace is a global domain, and this group lacks jurisdiction over foreign Internet Protocol (IP) space.

Third, counterintelligence (CI). This is a potential sweet spot in national cyber defense, as CI examines both internal and external threats. Still, CI also lacks legal jurisdiction overseas, and foreign intelligence usually outpaces this group with superior tools and tactics.

Given the collective limitations of these groups, world leaders may decide to give the responsibility for protecting their national IP space to militaries. After all, if enemy planes or tanks cross the border, it is the military that would fight them. So … if a military attacks another nation's public infrastructure (or even its private sector) with cyber attacks, who should take the lead on defense?

Different countries have different political philosophies, and different concepts of what is public and what is private. There are likely to be as many perspectives as there are nations. This debate is currently underway in Israel, with Prime Minister Netanyahu personally involved.

Militarization of the Net: ramifications

No president or general wants to explain how he or she lost a war due to poor planning or lack of preparation. Therefore, national leaders may give intelligence agencies and military units considerable freedom to prepare for the cyber wars of the future.

Their focus – both for offense and defense – will begin with the "hard targets": leadership communications, intelligence agencies, and weapons systems. Over time, more attention will be given to the "soft underbelly" of a nation – public critical infrastructure and the private sector.

From an attacker's perspective, undermining the security of hard targets requires an APT-level effort, and months if not years of painstaking subversion. On defense, protecting the computers and networks of large enterprises is also a full-time job.

The dilemma for national security planners is that if they wait until a national security crisis takes place, it may be too late – either to attack the enemy or to protect the homeland. The trouble is that some aggressive cyber war preparations will inevitably take place in peacetime, and may come at a high cost in terms of data privacy and human rights.

This troubling dynamic raises the following question: how much of the Internet is already occupied military ground?

I recently conducted an analysis of 18 months' worth of FireEye data, which included 30 million malware callbacks to 208 country

code top-level domains. Our most interesting finding was the discovery of a sharp rise in callbacks to three countries – Russia, Ukraine, and Israel – during the months they were engaged in war. The simple explanation, in my opinion, is that computer network operations are now an essential part of modern intelligence collection and military operations – and with a strategic data set to analyze, such operations can be hard to hide.

Conclusion: the future

There is only one Internet, and we need to be able to trust it. However, the existence of only one Internet means that there is only one cyber battlefield. The same, vulnerable IT infrastructure is used to manage libraries, private companies, frontline troops, public critical infrastructure, and our personal lives. Today, students, spies, and soldiers all live and work in the same IP space.

By the way, this state of affairs not only allows governments to spy on students, but students to spy on governments; students can write academic papers about real cyber espionage, and real cyber war. :)

As we can see from current events in the Middle East and Former Soviet Union, nations still wage wars. Therefore, their militaries will prepare today for the wars of tomorrow.

For the foreseeable future, traditional military might is still the ultimate defense of any country – but over time, computer network operations will play an increasing role in war. And some of the preparations for cyber war will include the peacetime occupation of strategic terrain on the Internet.

This militarization of the Internet – in peacetime – has significant ramifications for international cyber security, in part because the future is hard to predict, to include the next national security crisis. It will be hard to avoid some abuses of data privacy and human rights – which may be considered justifiable “friendly fire”.

The need to strengthen global cyber security against this emerging threat is clear, but it will take time. Cyber security

is a broad concept, and encompasses both tactical and strategic considerations.

Investment must begin at the tactical, technical level. The most important thing is to train more people in the science – and art – of information security.

Investment must continue at the strategic level. Traditional security concepts like deterrence, arms control, and proportionality in response are challenged by cyber-specific idiosyncrasies, including attribution, asymmetry, code inspection, and even a definition for what constitutes an attack.

Fundamentally, cyberspace is an international domain, so having traditional geopolitical allies is critical. In this light, I think the best places to look for improvement in international cyber security are in the European Union and in the North Atlantic Treaty Organization (NATO) – as they are the strongest political and military alliances in the world.

For our common future: government, the private sector, and individual citizens must work together in a mature way, based on the rule of law. But unfortunately, the world is filled with immature political systems.

Governments will never willingly disallow law enforcement, counterintelligence, foreign intelligence, and militaries the best tools to do their jobs. However, all of these organizations will make mistakes, overstep their bounds, and abuse the rights of citizens. Depending on the country, this could happen thousands of times – every day.

I believe the most important thing for strategic cyber security is to strengthen transparency and accountability in governments worldwide. And it is the Internet itself that provides us with the best mechanism to do this. That is why we must resist unreasonable government oversight – and the unnecessary militarization – of the Net.

References

Stoll, C. *The Cuckoo's Egg*, Doubleday (1989).

"Curtis LeMay", Wikiquote
http://en.wikiquote.org/wiki/Curtis_LeMay.

Molinaro, Kristin, "Infantry leaders sharpen training tactics to meet battlefield demands", *The Bayonet* (15 Sep 2010)
http://www.army.mil/article/45200/Infantry_leaders_sharpen_training_tactics_to_meet_battlefield_demands/.

Ravid, Barak. (21 Sep 2014) "Battle move in Israel's cyber turf war: Shin Bet loses authority over 'civilian space'", *Haaretz*
http://www.haaretz.com/news/national/1.616990.