ATLANTIC COUNCIL

IDEAS. INFLUENCE. IMPACT.

The Lessons of Cyber Conflict History, So Far…

Even in its earliest history, cyberspace had disruptions, caused by malicious actors, which have gone beyond being mere technical or criminal problems. These cyber conflicts exist in the overlap of national security and cybersecurity, where nations and non-state groups use offensive and defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes.[1] This book – meant both for national security professionals to understand cyber conflict as well as for cyber specialists to learn the national security context – is the only major attempt in twenty-five years to codify this history.

"**Cyber Wake-Up Calls**" (so far):

1. Morris Worm
2. ELIGIBLE RECEIVER and SOLAR SUNRISE
3. MOONLIGHT MAZE
4. Chinese Espionage
5. Estonia and Georgia
6. BUCKSHOT YANKEE
7. Stuxnet

There have been at least seven major "wake-up calls." Each shocked and surprised the defenders and decision makers that suffered through them, but their lessons were soon forgotten until a new generation of cyber leaders were again "awakened" to a similar shock.

In other areas of national security, new military personnel, diplomats, and policymakers are taught to avoid old mistakes thorough formal study of history thereby gaining the vicarious experience of those that have gone before. Just as we teach young cadets and military officers the implications of Gettysburg, Inchon, Trafalgar, and MIG Alley, so too must we pass along the lessons of past cyber conflict. Yet the opposite has been the case.

[1] "Cyber conflict" is meant to be more inclusive than "cyber war" which implies operations that cross a thresholdinto "armed attack." Cyber conflict excludes most cyber crime which is conducted for criminal, material gain not political purpose but can include the largest malicious Internet disruptions. For more, see Cyber Conflict Studies Association, "Addressing Cyber Instability," 2012 and the glossaries on the next page and in the appendix.

Cyber history has been forgotten, ignored as irrelevant, or even intentionally falsified even as a crush of new personnel storms into the field. Even the most historically minded of cyber warriors seem to spend more time wondering how, twenty-two hundred years ago, a southern Mediterranean general could get some elephants across the Alps than seeking lessons from KGB-tied intrusions into military networks merely twenty five years ago.

Moreover, the US government and military have almost completely ignored cyber history. Before being interviewed for this book, many of the cyber pioneers had never before been asked about those first organizations and conflicts and the lessons for today. Army Cyber Command is now teaching that the main cyber threat facing the nation prior to 2007 was "Cyber 'Noise' on Networks," ignoring two decades of teachable lessons.[2]

In fact, there is a rich cyber history prior to 2007 which is more than just noise. This history is not a collection of empty facts, trivia for cyber operators to play on a long night shift, but yields rich lessons. The most important of these lessons contradict much of which passes for perceived wisdom in today's cyber community. By ignoring history, the United States has learned the wrong lessons, leading to misunderstandings which could prove disastrous. Indeed, since they do not look backwards, today's practitioners may not understand how little progress has been made over the decades. As the comparative quotes in the text box show, to a large degree, the issues faced today are reflected in, or even exactly the same as, those faced by an earlier generation. If thirty years of dedicated work have not solved cyber problems, it's unlikely that we'll make a breakthrough if we continue to approach them with similar strategies and techniques.

As summarized in Table 1, cyber conflict history can be divided into three very distinct periods: *Realization* started in the mid-1980s, *Takeoff* in 1998, and *Mobilization* in 2003.

[2] Army Cyber Command Update, 8 March 2012, slide 3, http://www.afceabelvoir.org/images/uploaded/AFCEABelvoir_ARCYBERCommandBrief_COLSchilling_23APR12.pdf.

Table 1: Phases of Cyber Conflict History

	Realization	**Takeoff**	**Mobilization**
Start Date	1980s	1998-	2003-
Dynamics	O>D: Attackers have advantage over defenders	O>D: Attackers have advantage over defenders	O>D: Attackers have advantage over defenders
Capabilities	US and Few	Russia and Many	China and Everyone
Adversaries	Hackers	Hacktivists, Patriot Hackers, Virus and Worms	Neo-Hacktivists, Espionage, Malware, and Proxies
Major Incidents	Morris worm (1988), Cuckoos Egg (1989), Dutch hackers (1991), Rome Labs (1994), Citibank (1994)	Eligible Reciever, Solar Sunrise, Moonlight Maze, ALLIED FORCE, Chinese Patriot Hackers	TITAN RAIN, Estonia, Georgia, Buckshot Yankee
Driving Policy	Various covering communications security, command and control warfare	PDD-63	HSPD-7/HSPD-23, NSPD/NSPD-54, CNCI
Defense	CERT, NSA and AF Information Warfare Center (1993), and AF 609 IW Squadron (1995)	JTF-CND, JTF-CNO, USSPACE, NSA, CERT	JTF-GNO, USSTRAT / Cyber Command, DHS/NCSD, NCSC, NSA and USCERT
Offensive	Potential SAP programs	JTF-CNO, USSTRAT	JTF-CNO became JFCC-NW, USSTRAT
Coordination	IOTC, CERT, JTRB	IOTC, NIPC, and ISACs	NCRCG, SCCs, ISACS, USCERT
Doctrine	Information Warfare	Information Operations	Cyber
US Governance	Some NSC	J-39, NSC, PCIPB	National Security Council

Doomed to Repeated History

Reading quotes from thirty years of cyber security and conflict helps reveal how little progress has been made. Which quotes below are from our past and which are contemporaneous? Why can't we even tell the difference?

1	I liken it to the very first aero squadron when they started with biplanes. We're at the threshold of a new era . . . We are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know that we are the beginning.	I almost feel like it's the early days of flight with the Wright Brothers. First of all you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time and it's going to be growing.
2	Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.	[Our red teams] do get into most of the networks we target.
3	The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.	We've had market failure when it comes to cybersecurity. Security doesn't come out of voluntary actions and market forces.
4	[C]omputer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses … account for the largest portion of economic and industrial information lost by US corporations.	Cyber tools have enhanced the economic espionage threat, and the Intelligence Community judges the use of such tools is already a larger threat than more traditional espionage methods.
5	Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations … insulated from risks of internationally embarrassing incidents	Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets.
6	The almost obsessive persistence of serious penetrators is astonishing.	[The Advanced Persistent Threat] successfully evade anti-virus, network intrusion detection and other best practices.

The quotes in the First Column are at least fifteen years old: (1) Then Lt Col Dusty Rhoads in 1996, (2) Then Lt Col Roger Schell in 1979 (3) National Academy of Science repot, *Computers at Risk* in 1991 (4) NACIC counterintelligence report to Congress for FY95, (5) and (6) Cliff Stoll, "Stalking the Wily Hacker" in 1988

The Second Column are taken from quotes dating after 2008: (1) Maj General Webber, Comments at 2009 Air Force National Symposium 2) NSA red teamer, 2008 (3) Deputy Secretary of Defense Ashton Carter at the RSA Conference in 2012 (4) and (5) NCIX counterintelligence report to Congress, 2010, (6) Mandiant M-Trends, 2010

Lessons and Findings from Our Cyber Past

Even in an initial history of cyber conflict, key lessons and findings clearly emerge, each of which has significant policy implications for cyber defenders and policymakers today. As with any other lagging indicators, these help confirm the long-term trend, but cannot predict the future with accuracy.

1. **Cyber conflict has changed only gradually over time, making historical lessons especially relevant (though usually ignored).**

    a. There has been in fact no essential discontinuity between cyber conflicts of fifteen or twenty years ago and those of today. The dynamics of today's conflicts would be familiar to cyber defenders from those early days.

    b. Many of the questions vexing cyber policymakers today were asked in almost exactly the same terms by their predecessors ten or twenty years earlier. Again and again, lessons have been identified and forgotten rather than learned.

2. **The probability and consequence of disruptive cyber conflicts has been hyped while the impact of cyber espionage is consistently underappreciated.**

    a. The most important conflicts have not been not cyber war or cyber terror, but espionage.

    b. We have been worrying about a "cyber Pearl Harbor" for twenty of the seventy years since the *actual* Pearl Harbor.

    c. No one is known to have died from a cyber attack.

    d. There have so far been no massive attacks, no attacks causing even the smallest blip to national GDP, and little evidence of nations seeking to cause significant damage to each other.

    e. Cyber incidents have so far tended to have effects that are either (1) widespread but fleeting or (2) persistent but narrowly focused. No attacks, so far, have been *both* widespread and persistent.

f. As with conflict in other domains, cyber attacks can take down many targets, but *keeping* them down over time in the face of determined defenses has so far been out of the range of all but the most dangerous adversaries.[3]

g. Strategic cyber warfare has so far been far out of the range of the stereotyped teenage hackers in their basement.

h. When it comes to damaging cyber attacks (i.e., not espionage), adversaries typically *either* have the capability to cause significant damage or the intent to do so – but rarely have *both* dangerous capabilities and truly malicious intent.

3. The most commonly held views of strategically important cyber conflicts are so distant from their fundamental nature as to constitute myth.

a. Strategically meaningful cyber conflicts rarely occur at the "speed of light" or "network speed." While tactical engagements can happen as quickly as our adversaries can click the Enter key but, just as in traditional warfare, cyber conflicts are typically campaigns that take weeks, months, or years of hostile contact between adversaries.

b. Nations seem extremely reluctant to conduct damaging attacks to one another outside of traditional geo-political conflict.

c. Neither have terrorist groups yet chosen cyber attack as a primary attack. There have been no digital Pearl Harbors, no cyber 9/11s yet.

d. Because significant attacks are tied to geo-political conflicts, there is usually ample warning, even without relying on technical means.

e. While some attacks are *technically* difficult to attribute, it is usually much more straightforward to determine the nation responsible for the most disruptive or long-duration conflicts.

[3] This is most likely to change as nations put online more physical infrastructure, such as the Smart Grid.

f. Few cyber conflicts have been resolved by governments. It has been non-state actors – companies, volunteer groups – that have the most levers and are at the center of the defense.

These lessons show the underlying continuity of cyber conflict with traditional international relations, national security, and military operations. While there are certainly differences, so far it is simply not true that cyber conflicts have been *fundamentally* different from conflict on land, sea, air or space.

Moreover, these key historical findings are different from the common myths of cyber conflict imagined as massively disruptive lightning wars unleashed either by kids in the basement or nations with surprise attacks totally unlinked to geopolitical tensions. While not impossible, it has not yet happened.

The US failure to notice these lessons and learn from them has critical implications for cyber operations today and tomorrow. For example, cyber conflict is fast but by no means at the "speed of light" or even "network speed" as described by US military leaders. As later sections of this history will discuss, MOONLIGHT MAZE, Estonia, Conficker, Stuxnet, and Chinese cyber espionage were all prolonged conflicts. The focus of the US cyber community on this single mistaken point means it will likely over-invest in capabilities and doctrine to automatically counterattack against surprise attacks. Rules of engagement will allow ever-lower levels to shoot back without seeking authorization -- a relaxation of the rules which may not be in the long-term US economic or military interest. Response plans will focus on today's incident, with little thought on how to surge and sustain an effort over the weeks and months over which conflicts have occurred. Defensive actions which make sense in longer campaigns (such as installing new networking capabilities and Internet Exchange Points) will be ignored.

Likewise, the US national security community should know it is difficult to have a prolonged strategic effect, even in cyberspace. If Flying Fortresses in World War Two could not achieve a

strategic victory over Germany after dropping millions of tons of high explosives over several years of operations, why do so many people still believe that a few kids might take down the United States from their basement?

Yet basement-originated strategic warfare is a common theme, as recently as March 2012, the four-star general who heads up Air Force Space Command told a cyber futures conference that deterrence was difficult in cyber conflict since, "For someone with the right brainpower and the right cyber abilities, a cheap laptop and Internet connection is all it takes to be a major player in the domain."[4] These tools might help an adversary steal data or identities – even conduct a major intrusion – but they are not sufficient for a strategic effect that requires deterrence power from the world's most powerful military.

[4] General William Shelton, Commander Air Force Space Command, remarks at Air Force Association, CyberFutures Conference, 22 March 2012. Audio available at http://www.afa.org/events/CyberFutures/2012/postCyber/default.asp (quote around 14:47).