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 were greater than mere technical or criminal problems. These cyber conflicts occurred in the overlapping area between national security and cyber security, wherein nations and non-state groups used offensive and defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes.[1]

This paper discusses the main lessons from this history, based on a forthcoming book which examines the first twenty-five years of cyber conflicts. *A Fierce Domain, Cyber Conflict from 1986 to 2012* will be out in the Summer of 2013. A joint effort by the Atlantic Council and Cyber Conflict Studies Association it is is the only major attempt 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 wave of cyber leaders were again "awakened" to a similar shock.

In other areas of national security, new military personnel, diplomats, and policy makers are taught to avoid old mistakes through a formal study of history. They thereby vicariously gain the 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

[1] "Cyber conflict" is a term that is meant to be more inclusive than "cyber war," which implies operations that cross a threshold into "armed attack." Cyber conflict excludes most cyber crime, which is conducted for criminal and material gains, but not for political purposes. Cyber conflict can include the largest, malicious Internet disruptions.

along the lessons of Cookoo's Nest, the Morris Worm, and Stuxnet. Yet the opposite has been the case.

Cyber history has been forgotten, ignored as irrelevant, or intentionally falsified, just as a crush of new personnel floods 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, rather than seeking lessons to be learned from KGB-associated intrusions into military networks, which happened a mere twenty-five years ago.

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 the first cyber organizations and conflicts, or about their ideas concerning lessons for today. A recent search for "cyber" on an official historical site maintained by the Air Force led to only four documents, no images, and a single video (which was from 2012; this hardly counts as historical).[2] Army Cyber Command is now teaching that the main cyber threat which faced the nation prior to 2007 was "Cyber 'Noise' on Networks." This ignores two decades of cases and derivable lessons.[3]

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, nor trivia for cyber operators to recall for amusement on a long night shift. It yields rich lessons. The most important of these lessons contradict much of which passes for received wisdom in today's cyber community.

By ignoring history, the United States has learned (and is now learning) the wrong lessons. This situation has generated misunderstandings that could prove disastrous. Most cyber conflicts

[2] The search was conducted on http://www.airforcehistory.af.mil/main/welcome.asp in July 2012.
[3] Army Cyber Command. "Army Cyber Command Update," March 8, 2012, slide 3.

are more than mere, scaled-up hacking attempts, which are often associated with dark and technical mysteries, uncertain attributions, and "speed of light" executions. The reality is that the more strategically significant cyber conflicts of the past have been similar in their dynamics to the more familiar types of conflict that occur on the land, in the air, or on the sea. Significantly, the most important difference between them is regularly ignored. This difference is that the private sector, not governments, plays the primary role in cyber conflicts.

Since today's practitioners rarely look backwards, they may not understand how little progress defenders have made over the last few decades. As the compartative quotes which appear below demonstrate, to a large degree the issues faced today are largely reflected in, or are exactly the same as, those faced by the previous generation. Since twenty-five years of dedicated work has not solved cyber problems, if we continue to approach them with the same old strategies and techniques, it is unlikely that we will be any more successful.

As shown in Table 1, cyber conflict history can be divided into three very distinct periods. *Realization* started in the mid-1980s, *Takeoff* in 1998, and *Militarization* began in 2003. Each of these periods will be examined in the following pages. In each period, policy makers and technical experts struggled with a few key questions. Are we being too paranoid, or not nearly paranoid enough? How much do we focus on fighting crime, stopping espionage, or defending against catastrophic attacks? What is the right balance between offense and defense? How do we coordinate between different agencies and countries? What is the proper role for the private sector?

This discussion will examine how all of these questions have been answered in the past. But we will start with the conclusions drawn from all of this: the lessons and findings gleaned from an understanding of cyber conflict history.

Table 1: Phases of Cyber Conflict History

	Realization	Takeoff	Militarization
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
Who Has Capabilities?	US and a few others	US, Russia, and Many	US, Russia, China, and many, many more
Adversaries	Hackers	Hacktivists, Patriot Hackers, Viruses, and Worms	Neo-Hacktivists, Espionage agents, Malware, National Militaries, Spies, and their Proxies, Hactivists
Major Incidents	Morris Worm (1988), Cuckoos Egg (1989), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Maze ELIGIBLE RECEIVER, SOLAR SUNRISE, MOONLIGHT MAZE, ALLIED FORCE, Chinese Patriot Hackers	TITAN RAIN, Estonia, Georgia, BUCKSHOT YANKEE
Driving Policy / Policies	Various covering communications security, command and control warfare	PDD-63	HSPD-7/HSPD-23, NSPD/NSPD-54, CNCI
US Defense Organizations	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, NSA, and USCERT
US Offensive Organizations	Special Access Programs	JTF-CNO, USSTRAT	JFCC-NW, USSTRAT, US Cyber Command
Coordination Organizations	IOTC, CERT, JTRB	IOTC, NIPC, and ISACs	NCRCG, SCCs, ISACS, USCERT
US 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 history helps to reveal how little progress has been made in cyber conflict awareness. Which quotes below are from our past and which are more contemporaneous? Why is it hard to 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 [that] 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 … [while the perpetritors are] 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."

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

The Second Column quotes date from after 2008: (1) Maj. Gen. 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, and (6) Mandiant M-Trends, 2010.

LESSONS AND FINDINGS FROM OUR CYBER PAST

From the history of cyber conflict, key lessons and findings clearly emerge, and each of these carry significant policy implications for cyber defenders and policy makers today. As with any other indicators, these observations help confirm the long-term trends, but cannot be depended upon to predict the future with accuracy.

1. **Cyber conflict has changed only gradually over time; thus, historical lessons derived from past cases are still relevant today (though these are usually ignored).**

    a. Conflicts today are not exact repetitions of past events, but they are clearly echoes.

    b. There has been no essential discontinuity between the cyber conflicts of twenty-five years ago and those of today. Technologies have changed, but the underlying dynamics of today's conflicts would be familiar to cyber defenders from those early days.

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

2. **The probability and consequences of disruptive cyber conflicts have often been hyped, while the real impacts of cyber intrusions have been consistently under-appreciated.**

    a. Historically, the most important cyber conflicts have not involved war or terror, but rather espionage.

    b. However, it is increasingly clear that nations, including the United States, are engaging in covert "shadow conflicts," which is irregular warfare using proxies and covert sabotage.

    c. Cyber espionage against the United States has been occurring since at least the mid-1980s. But today it is far, far worse–indeed, some say intolerable. Of course, the United States is extremely active in its own, quieter cyber espionage.

d. While the cost of espionage is high (but difficult to estimate, much less to calculate), there is little evidence that disruptions have caused even blips in national GDP statistics.

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

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

g. Nations have not sought to cause massive damage to each other outside of larger geo-political conflicts.

h. Cyber incidents have so far tended to have effects that are either widespread but fleeting, or persistent but narrowly focused. No attacks, thus far, have been *both* widespread and persistent.

i. 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 thus far been beyond the capabilities of all but the most dangerous adversaries.[4]

j. Strategic cyber warfare has thus far been well beyond the capabilities of stereotyped, teenaged hackers in their basements.

k. Adversaries historically have had *either* the capability to cause significant damage *or* the intent to do so—but rarely did they possess *both* dangerous capabilities *and* truly malicious intent.

3. The more strategically significant a cyber conflict is, the more similar it is to conflicts on the land, in the air, and on the sea – with one critical exception.

a. The most meaningful cyber conflicts take weeks, months, or years of hostile, back-and-forth action between adversaries, and rarely occur at the "speed of light" or "network speed."

[4] This will likely change as nations put more physical infrastructure online, such as the Smart Grid.

b. While tactical engagements can happen as quickly as our adversaries can click the Enter key, cyber *conflicts* are typically campaigns that encompass weeks, months, or years of hostile contact between adversaries, just as in traditional warfare.

c. Because the most strategically meaningful cyber conflicts have been part of larger geo-political conflicts, their nature has tended to offer ample warning time to defenders, even without reliance on technical means. A good rule of thumb is that "physical conflict begets cyber conflict."

d. While some attacks are *technically* difficult to attribute, it is usually a straightforward matter to determine the nation responsible, since the conflict takes place during an ongoing geo-political crisis.

e. There have been no digital Pearl Harbors yet. Nations seem generally reluctant to conduct large-scale damaging attacks on one another, outside of traditional geo-political conflicts.

f. To date, no terrorist groups have chosen cyber attack as a primary attack method. There has been no Cyber 9/11 yet, a major attack designed to cause death, destruction, and terror.

g. Perhaps the biggest difference between cyber conflicts and their traditional equivalents is the one most often overlooked: when defending against cyber conflicts, it is non-state actors, not governments, which play the key role. Companies and volunteer groups have repeatedly used their agility and subject matter knowledge to mitigate and prevail in most of the conflicts in this book, while governments are on the side. Only uncommonly are governments able to bring the superior resources of their unwieldy bureaucracies to bear in enough time to make a significant difference to defensive efforts.

Despite the popular conception that the nature of cyber "war" must constantly change with every new technology, this book makes the case that the situation is happily much different. The lessons from yesterday are not trivia–they remain eminently useful.

As an analogy, imagine buying a few rounds of drinks for a modern fighter pilot of an F-22 Raptor, and at the same time, for some of his predecessors from World Wars One and Two. Despite over a hundred years of technological and doctrinal changes between their respective careers, within five minutes they would be telling breathless tales of dogfights, and how they had zipped through complex aerial maneuvers to lose an adversary or to line up a kill shot. The dynamics of dogfighting, such as the advantages of relative height, speed, and manuerability, have remained stable over time, even though technology has made dogfights faster, higher in altitude, wider in range, and above all, more lethal. So it is with cyber conflicts.

In addition, these lessons show the underlying continuity of cyber conflict with traditional international relations, national security, and military operations. While there are certainly differences, to date cyber conflicts have not been *fundamentally* different from conflicts on the land, in the air, or on the sea.

The key historical findings above are different from the common myths about cyber conflict, such as that cyber attacks are like massively disruptive, lightning wars unleashed either by kids in their basements or by nations using surprise attacks which are wholly unrelated to current geopolitical tensions. While not impossible, these scenarios have not yet materialized.

It appears that cyber deterrence, long the subject of theory but usually dismissed, has been practiced for some time. This has gone unrecognized, because historical analysis has been focused on quotidian hacking and technical details, rather than on conflicts as nations have actually conducted them.

Despite early fears that nations would strike at each other using surprise, strategic attacks, while relying on anonymity within the Internet, there is no evidence that such conflicts have occurred. Nations seem to be willing to launch significant cyber assaults during larger crises, but not out of the blue. Accordingly, a comparison with nuclear deterrence is extremely relevant,

but not necessarily the one that Cold Warriors have recognized.

Nuclear weapons did not make all wars unthinkable, as some early Cold War thinkers had hoped. Instead, they provided a ceiling under which the superpowers fought all kinds of wars, regular and irregular. The United States and the Soviet Union, along with their allies, engaged in lethal, intense conflicts ranging from Korea to Vietnam, and through proxies in Africa, Asia, and Latin America. Nuclear warheads did not stop these wars, but they did set an upper threshold which neither side proved willing to cross.

Likewise, though the most cyber-capable nations (including the USA, China, and Russia) have been more than willing to engage in irregular cyber conflicts, they have stayed well under the threshold of conducting full-scale strategic cyber warfare, and have thus created a *de facto* norm. Nations have proved just as unwilling to launch a strategic attack in cyberspace as they have been to do on the land, in the air, or on the sea.

The failure of the United States to learn from these lessons, or indeed even to notice that there is a history from which they may learn, has critical implications for cyber operations today and tomorrow. For example, cyber conflicts are fast, but by no means do they occur at the "speed of light" or even at "network speed," as is routinely 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.[5]

Tactical engagements in every domain can unfold quickly (for example, aerial dogfights in every war could sometimes be over before an unsuspecting pilot knew he was in one), but successful generals and strategists never allow themselves to obsess over these tactical engagements.

[5] Since this book is in part a military history, the US military format of writing military exercises and operations in all capital letters has been followed, e.g., MOONLIGHT MAZE.

Instead, they extrapolate from each action to more strategic levels to plot several moves ahead. This will be difficult if we continue to over-emphasize tactical, rather than strategic, truths.

These popular misunderstandings of cyber conflicts have critical implications, which include the following.

1. The US cyber community will likely over-invest in capabilities and doctrine to automatically counterattack against surprise attacks.
2. Rules of engagement will allow ever-lower levels of military authority to "shoot back" without seeking authorization—a relaxation of the rules which may not be conducive to long-term US economic or military interests.
3. Response plans will focus on today's incident, with little thought on how to surge and sustain an effort over the weeks and months that it has previously taken conflicts to occur.
4. Defensive actions which make sense in longer campaigns (such as installing new networking capabilities and Internet Exchange Points) will be ignored.
5. The US military will train their new cyber cadres with doctrines and strategies that are focused only on the immediate fight, with little conception of the true nature of the strategic whole.

A reading of today's headlines shows that the US military is barreling down most, if not all of these roads.

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 garage or basement?

Yet basement-originated strategic warfare is a common theme. As recently as March 2012, the four-star general who oversees Air Force cyber operations said at a conference that deterrence was difficult in cyber conflict since, "[f]or 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."[6] These tools might help an adversary to steal data or identities—or even to conduct a major intrusion. But they are not sufficient for a strategic effect that requires deterrence power from the world's most powerful military.

At least as important is the principal difference between cyber and traditional conflicts: the primacy of the private sector. Cyber conflict history clearly shows that nearly every significant incident has been resolved by the private sector, not the government. Yet government response plans, such as the US National Cyber Incident Response Plan, reverse this emphasis and discuss how government bureaucrats and elected officials will make the key decisions. In cyber conflicts, the private sector is not a "partner" of government, but the "supported command."

Excerpted from the introduction of

A Fierce Domain: Cyber Conflict 1986 to 2012

Jason Healey, editor

DRAFT, 15 April 2013

[6] Shelton, remarks at Air Force Association, CyberFutures Conference, March 22, 2012.