CHAPTER

16

The Future of Cyber War

INFORMATION IN THIS CHAPTER

- Predicting the Future
- Emerging Trends
- Trends Driving Where We Will Go

When we think of how the science fiction stories in the 1970s predicted one computer the size of Texas would control centrally everything it is easy to see how impractical predicting the future is. At the time it was a natural extension of how the mainframe computers of the day would evolve, but then came the personal computer and everything changed. However, now that the trend is shifting to cloud computing, where we leverage large data centers; who knows, maybe they had it right after all. Surprise is the enemy of national strategies, so how do we avoid or survive it. First, let us start by looking at a couple of theories that might help—the impact of Black Swan events and the Air Force study on how to minimize the impact of Capability Surprises, revelations in military affairs and catalysts events.

The Introduction of *The Black Swan: The Impact of the Highly Improbable* offers a great description:

> Before the discovery of Australia, people in the old world were convinced that all swans were white, an unassailable belief as it seemed completely confirmed by empirical evidence. One single observation can invalidate a general statement derived from millennia of confirmatory sightings of millions of white swans. All you need is one single black bird. What we call here a Black Swan (and capitalize it) is an event with the following three attributes. First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable. I stop and summarize the triplet: rarity, extreme impact, and retrospective (though not prospective) predictability [1].

This section of the book points out the challenge of predicting cyber warfare from both long-term evolution and sudden paradigm shifts.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00016-7

It is also worth looking at the condensed version of the ten principles for a Black Swan-proof world [2] based on our recent housing financial crisis. Following this philosophy will lead to an economic life closer to our biological environment: smaller companies, richer ecology, and no leverage. A world in which entrepreneurs, not bankers, take the risks and companies are born and die every day without making the news. In other words, an economy more resistant to Black Swans. These principles are built around a different problem but can be used as an example to develop similar rules for cyberspace. We need a framework that is resilient to Black Swans. Here are the areas epistemologist and author of the book *The Black Swan: The Impact of the Highly Improbable* Nassim Taleb suggests we focus on as we look at the economy:

1. What is fragile should break early while it is still small.
2. No socialization of losses and privatization of gains.
3. People who were driving a school bus blindfolded (and crashed it) should never be given a new bus.
4. Do not let someone making an "incentive" bonus manage a nuclear plant—or your financial risks.
5. Counter-balance complexity with simplicity.
6. Do not give children sticks of dynamite, even if they come with a warning.
7. Only Ponzi schemes should depend on confidence. Governments should never need to "restore confidence."
8. Do not give an addict more drugs if he has withdrawal pains.
9. Citizens should not depend on financial assets or fallible "expert" advice for their retirement.
10. Make an omelet with the broken eggs; do not try to patch them.

Next, we have the *Defense Science Board publication discussing Capability Surprise* report. This report was designed to address the need for our military to be prepared to deal with the shock of new abilities or technologies that could impact national power. Capability Surprise can spring from many sources: scientific breakthrough in the laboratory, rapid fielding of a known technology, or new operational use of an existing capability or technology. A review of many surprises that occurred over the past century suggests that surprises tend to fall into two major categories: (1) "Known" surprises—those few that the United States should have known were coming, but for which it did not adequately prepare. (2) "Surprising" surprises—those many that the nation might have known about or at least anticipated, but which were buried among hundreds or thousands of other possibilities [3]. The most recent examples would be the announcement of two jets: the Russia's stealthy PAK-FA [4] and China's fifth-generation J-20 stealth fighter [5]. These capabilities were not expected as soon as they were developed and could change the balance of air power.

As we look at the framework for handling cyber surprise in the context of strategy, plans, and preparations, we see it also provides an assessment of current readiness. Three cases are addressed (see Table 16.1 for details):

1. Prevent surprise (influence, uncover, eliminate)
2. Deal with surprise (stabilize, mitigate, recover)
3. Create surprise (adapt, reverse, reshape)

TABLE 16.1 Sample Managing Cyber Surprise Framework [3]

Strategy	Plans	Preparation
Prevent surprise (influence, uncover, eliminate)	Deal with surprise (stabilize, mitigate, recover)	Create surprise (adapt, reverse, reshape)
Understand adversary's capabilities and intentions	Detect attack	Support IO through cyber deception
Keep cyber assets and capabilities within the U.S.	Plan/exercise with varying degrees of degradation	Prevent enemy actions through cyber intervention
Assure hardware and software provenance throughout lifecycle	Reconfigure and reallocate resources	Co-opt cyber attacks
Deter attacks	Capture forensics data	
Defend the network		
Strengthen robustness		

Of the 16 capabilities examined during this report we used the traditional stoplight naming convention of green being in good shape, yellow having concerns, and red being broken. As the capabilities ranked two were considered "green" (satisfactory), five were "red" (unsatisfactory), and the rest "yellow" (not ready, but some progress being made).

So understanding there will be Black Swan events, and some of them can come in the form of surprises in our adversary's capabilities, it becomes more important to keep a close eye on how trends and new technology will impact cyberspace. The sooner we recognize the change and begin to respond, the easier it is to adjust strategies and reorient resources.

These changes are often driven by technology. Technical advancements have had impacts on tactics, policy and strategy of warfare throughout history. Some, like gunpowder, nuclear bombs, and space platforms, have caused a "Revolution in Military Affairs" (RMA), also known as "Military Technical Revolutions." Others have caused paradigm shifts in organizational structures and doctrine such as airplanes, submarines, and machine guns. Some innovations have been transformational like stirrups, precision strike munitions, and radios. Some inventions were designed for the military while others like internal combustion engines, railways and information technology advances were leveraged by it. Some of these technological changes were incremental, like the machine gun being a natural evolution to increase the rate of fire for rifles. Others reflect the concept of Black Swans [6] or the parallel idea—Dragon Kings [7] (when diverse elements on the internet self-organize their internal structure and their dynamics with novel and sometimes surprising macroscopic "emergent" properties disrupting current relationships of influence or power) where there is dramatic surprise about the change. Cyber warfare has undergone transformation under all these aspects of change.

Cyber warfare has undergone changes in what has been called, including Electronic Warfare, Information Superiority, Information Dominance, Network Centric Warfare, Information Warfare, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), Hyperwar, Netwar, and Third Wave Warfare. These terms generally refer to conflicts in the cyber domain. Cyber is separate from other RMAs ongoing today in unmanned aerial vehicles or drones, nanotechnology, robotics, and biotechnology.

Cyber is built on a physical infrastructure but is unique in that it has a virtual component. It is also prone to more rapid shifts since software is developed at a much faster pace than hardware. Technology will continue to drive change in society, economies, and warfare. We will start by looking at some of the changes that have impacted the Internet in general.

As a baseline we have provided a timeline of the major events along the cyber timeline (see Appendix). This is a good format to look for paradigm shifts in both security and threats as well as where we seem to be stuck in a paradox experiencing the same issues year after year. We will see that while at the time of an event many of us believed it to be significant, many seem to have had no long-term impact. There are some major evolutionary events and a few with revolutionary impact. As a sample we would point to 1988 when the Morris worm should have been a wake-up call for security, but in 1999 we see the same thing when the Melissa virus hit, then again in 2004 when LoveLetter caused havoc. These show a pattern of the military and the IT industry ignoring the fundamental security issues that allowed these worms and viruses to spread. Some major (but still evolutionary) events in cyber conflicts are the 2004 Supervisory Control and Data Acquisition (SCADA) attack on the Russian pipeline [8], 2007 attacks on Estonia [9], the 2008 agent.btz intrusions which resulted in operation Buckshot Yankee [10] and the cyber attacks against Georgia during conflict with Russia [11]. In 2010 we had Operation Aurora against Google (which has both counter intelligence and intellectual property theft aspects) [12] and Stuxnet SCADA [13] attacks. These events show an increasing use of cyber attacks with overtones of state sponsorship. In the revolutionary category there is ARPANET being stood up and social media exploding onto the net. These were events that created paradigm shifts in how we use the Internet and open up net threat vectors at the same time.

As we look at the potential threats, one way to categorize them is by the level of resources they commit [14]. There are some tier one nations that are committing billions of dollars to cyber warfare like the United States, China, and Russia. In McAfee's report "In the Crossfire Critical Infrastructure in the Age of Cyber War" executives from many nations, including many U.S. allies, rank the United States as the country "of greatest concern" in the context of foreign cyber attacks, just ahead of China [15]. At the next level there are countries and non-nation state actors like criminal organizations investing millions of dollars in developing and employing cyber tools. Finally, there are individual hackers or groups like Anonymous only spending a few dollars. Unfortunately, unlike conventional weapons development the potential impact of these organizations cannot be based on their resources alone. That said we will continue to see rapid increases in attack capability, many of which are designed to be stealthily or are classified.

NOTE

Every year we have a number of reports on the issues with our Critical Infrastructure (CI) but there is nothing driving the commercial companies that run our CI to invest in cybersecurity. In defense of the CI leadership, a simple question on return on investment would go something like this:

CEO: If we give you all the money you want to build the best cybersecurity possible could you guarantee our systems would be secure?

CISO: Nope, there could be a zero day exploit that we cannot protect against.

CEO: Then why should we invest more than the absolute minimum?

Another way to categorize potential threats is how they impact aspects of national power. These would be based on evaluating impact of attack/defend/exploit capabilities across Diplomatic, Information, Military, and Economic (DIME) elements of national power. Typically discussions on warfare focus on armies, weapons, and leadership but in today's conflicts we are seeing more integration of all these capabilities. The U.S. Secretary of Defense is talking about both cyber and the national debt today. DIME presents a solid way to evaluate the multiple aspects of Internet-based activities that can be part of cyber warfare. The impact of intellectual property theft can be looked at as economic warfare when you consider the aggregated damage to a nation—but what about the impact of cybercrime? This chapter will review where cyber warfare is going based on these elements, but in the end we must devise a national formula that will ensure we are ready for the next conflict based on something like Aggregation of capabilities + Innovations + Resources + Leadership = Strategic Advantage.

Finally, we need to look at catalyst events like the Battle of Waterloo, Pearl Harbor, Hurricane Katrina, and 9/11. When many of us started out in security it was just the technicians talking about how the internet was going to enable Virtual Guerilla Warfare and create the parameters for an Electronic Waterloo, today it is the senior national leaders talking about a Cyber Pearl Harbor or 9/11. The terms we use to frame the discussion will to some degree determine the solution. If we are talking about a cyber Katrina or pandemic, it is very different than events that lead us into wars.

There are clearly two camps framing the argument over cyber warfare. On the "cyber-armageddon" side an unofficial spokesperson is Mike McConnell, former Director of National Intelligence, and currently a Senior Executive for a defense contractor, who wrote in Washington Post, "The United States is fighting a cyber-war today, and we are losing. It's that simple" [16]. On the "cyber war is hype" side there is Bruce Schneier who wrote a Cable News Network piece saying, "We surely need to improve our cybersecurity. But words have meaning, and metaphors matter. There's a power struggle going on for control of our nation's cybersecurity strategy, and the National Security Agency (NSA) and Department of Defense (DoD) are winning. If we frame the debate in terms of war, if we accept the military's expansive cyberspace definition of 'war,' we feed our fears. . . If, on the other hand, we use the more measured language of cybercrime, we change the debate. Crime fighting requires both resolve and resources, but it's done within the context of normal life. We willingly give our police extraordinary powers of investigation and arrest, but we temper these powers with a judicial system and legal protections for citizens" [17]. These statements still represent the general outline of the agreement today.

Are these positions diametrically opposed? One very interesting perspective and potential answer was from Lt. General Harry D. Raduege, USAF (Ret), Senior Counselor, The Cohen Group. He sees cyber warfare divided into war with a small "w" (think "war on drugs" or "global war on terror") and War with a capital "w" being a congressionally declared war (think back to WWII). This leads to the possibility on a strategic level of a "pure cyber War" or a War with major cyber implications. It would also break out today's "war on cybercrime" or "war on cyber espionage" as vital government operations involving all elements of national power but on a more operational or tactical level [18]. This would lead to clearly different levels of engagement and could bridge the gap between hype and Armageddon.

Another perspective is from Eugene Kaspersky, CEO and co-founder of Kaspersky Lab who provided the following statement:

> What is the difference between a full-scale war and a special-forces raid? The answer is obvious: the scope of the conflict. The same can be applied to the cyberworld. When I speak about cyberwar, I understand it as a permanent stand-off between states, with each country targeting the opposition's critical infrastructure in the form of cyberweapons. Luckily we haven't experienced a true cyberwar yet, and hopefully we never will. However, instances of cyber attacks that fall within the scope of a special-forces raid, such as Stuxnet, indicate the danger and inherent risks of these conflicts escalating into a full cyber war. A cyber war would be an extremely serious and critical event, with the potential to inflict significant damage to a country across all levels – national, corporate and civilian. An attack during a cyber war would be designed to cause physical damage to a country's critical infrastructure, including its energy, transportation and financial systems, telecommunications and government networks.
>
> Many countries understand the possibility of a cyber war and the capabilities of cyber weapons. The United States, China, United Kingdom, Germany, India and other countries have already implemented special units who are tasked with developing and protecting their country. However, it's extremely important to understand that a cyber war also introduces new risks and dangers that span beyond direct cyber-attacks targeted at opposing countries. Unlike traditional weapons, tools used in cyber warfare are very easy to clone and reprogram by adversaries or other threat actors. For example, it would be extremely difficult for a cyber terrorist group to steal an intercontinental ballistic missile and locate a launch pad to fire it. Even if they succeeded in this scenario, they would not be able to duplicate the missile unless they stole another one. These physical barriers are nonexistent with cyber weapons – they can easily be hijacked, reprogrammed, duplicated and launched in a series of sustained strikes. It's imperative for countries to understand the consequences, dangers and potential damages that cyber war imposes before developing and possessing offensive cyber weapons.
>
> I believe that there is only one way to save the world from cyber war – a non-proliferation agreement, similar to nuclear weapons, must be signed. I see two ways in which the world can move forward in the next decade. The first is dark and apocalyptic – an uncontrolled arms race will continue, and sooner or later a global cyber war will start. I cannot estimate the results of such a war, but I can definitely say that it will be extremely serious. The second direction is more optimistic. International collaboration and information sharing among nation's leaders will increase, resulting in a peaceful meeting where an international agreement is signed. I believe that common sense will prevail, leaving the cyber world's Pandora's Box safely locked up.
>
> There is a good chance there will be a cyber-catalyst event. It is quite possible if the general population was aware of the amount of intellectual property theft it could cause popular demand for action – the type of action could be determined by whether we called it cyber-crime, cyber industrial espionage or economic warfare. How we react to a catalyst event could allow us to take actions quickly that causes more damage in the long run. We could establish treaties that put us at a disadvantage or impose restrictions that take away our competitive advantages. On the other side of the argument is that our inaction will result in technological atrophy and we will not have the cutting edge technology or skilled cyber engineers/warriors needed to maintain our cyber health much less than the cyber national power parity we currently have.

This statement covers the challenge of defining a cyber war, the players and the need for international agreement and concern there will be a cyber-catalyst event. As we look across cyber experts from many different nations, we see there are a lot of common themes you will find throughout this book driving home the point that it's a shared problem we all face.

EMERGING TRENDS

In this section, we will address some of the recent events that will lead to some natural evolutionary trends. This is based on logical progression ignorant of the many factors that will impact what happens over the next few years. First, we will look at three events and

see what they may impart—Aurora, Stuxnet, and WikiLeaks. Aurora [19] was the breach of Google (among other companies) by Chinese hackers. This brought espionage into the headlines and ended in cooperation between a commercial company and NSA. These public/private partnerships will be key going forward, but the momentum seems to have fallen off quickly. An expansion of the number of companies that enter into a partnership with the federal government will help everyone. In the past, most companies have felt that it has been a one way street and the government has not been sharing much of what they have learned. The authors hope that this trend of sharing will increase and the government will address the need to share more. There are a number of programs and efforts working toward that end today. Next, we had Stuxnet [20], a piece of malcode that was reported by the New York Times to have been developed by the U.S. and Israel to attack a specific national capability to develop nuclear material in Iran. This brought cyber weapons into the headlines but, even though many of the news articles were worthy of a Hollywood action movie script, there seemed to be no national policy reaction to what could have been a targeted raid, show of force, or act of war. It did however create interest in how weaponized code could become rogueware, having unintended consequences, as some analysts believe it started attacking systems that were not part of the original target set. This trend will likely continue until some rules (official or unofficial) are developed to determine what level of cyber intrusion is acceptable. Finally, we have the WikiLeaks site exposing banking records and U.S. State Department cables [21] to name a couple of examples. This may be the first case of a new type of insider threat where whistleblowers now go straight to posting documents online. It will create a new need for data control management and insider threat programs. This form of exposing secrets could become a game changer if we see a sharp increase in the number of "authorized users" who start to post restricted, proprietary, or even classified information for altruistic reasons or because they have become disgruntled. These types of events seem to get a lot of play in the news but often do not turn into changes in how people, organizations or countries protect themselves.

NOTE

Moving at Cyber speed vs real world is an interesting problem. We know one human year is roughly equal to seven in a dog's lifespan. How do we measure cyber time? Some say we need to move at the speed of light (generally when talking about making decisions). Others that we need to move at the speed of need (mostly referring to acquisition). We have Moore's law that the number of transistors on a chip will double about every two years. For how quickly things are changing in social media it would seem one cyber month is equal to one human year. For legal or regulatory practices it might be more like one cyber minute is equal to one year of legislative activity. One concern we face is that we act like all these activities move at a constant speed rather than the relative speeds they really do. So do we take the human out of the loop and let machines react at cyber speed?

Some issues that seem to be on the radar with little progress despite their critical needed are: cybercrime, Critical Infrastructure Protection (CIP)/SCADA vulnerabilities, social networks, mobile devices (apps), information sharing and cloud computing.

Cybercrime is growing rapidly but still does not seem to have hit the level of pain needed to be addressed in a concerted way. There are a lot of agencies and companies fighting it but they

are all isolated efforts and the crime wave is unbroken. The unanswered question is what will it take to make this an international issue? The most likely course of action is cybercrime will follow the "drug war" program which has a lot of resources but does not seem to be getting much better either.

CIP/SCADA vulnerabilities is in the news and often part of national security discussions but there has been little change in policy. There is some confusion on which government agency owns the cybersecurity-related issues for the different critical infrastructures and what the role of government should be. In the U.S. there is not likely to be any legislation impacting how they are regulated in the next couple of years so any changes will be driven by user demands.

Even if we do secure our networks we have "social networking" activities, which open attack vectors through our users that bypass our network security infrastructure. Most organizations are not putting the effort into training their staff on how to practice due care when on websites like Facebook and Twitter, so we believe this issue will continue to grow. This issue ties into the next one which is the number of mobile devices users that are connecting to an organization's networks so they can do their work and manage their personal life at the same time. People have laptops, smart phones, thumb drives, and tablets to be more productive, and they use them without thinking about security. They continue to download applications to all these devices with no concern about the security or validity of the programs. There are also a lot of devices that are not necessarily mobile but are now connected to the Internet. Our cars can be remotely tracked; our houses will soon be able to be monitored to track our activities and our heating system and refrigerators have become connected. While we think of the advantages, the threat is busy thinking of new "business models" to take advantage of them. If we are mad at our neighbor we can turn off their heating system when they leave for work in the winter. If we want to sell more tune-ups we can remotely turn on the check engine light on the cars that use our garage. If we want to sell information on the people who live in a particular city we can track their electricity usage and sell the information to companies that sell solar panels so they would know who their best potential sales targets would be. This could be a threat to privacy or in the case of military personnel attack on OPSEC.

TIP

When thinking about how to protect our systems first we must determine what information is truly critical (i.e., to lose or have it compromised could cause irreparable damage), what is vital (e.g., things like email, web access, and resource management applications) and what we can do without (e.g., Instant Messaging and access to file servers with historical data and corporate policies). Once we know what is critical, we can build a security plan that employs the right tools and focus resources appropriately. It is time to stop protecting all the systems at the same level and increase the monitoring and protection of the critical data.

Cloud computing is becoming more prevalent, which brings benefits and new attack vectors. For most companies, running a network is a distraction and at some point it is natural to outsource things that are not part of the core business. Looking at a historical example of this, when electricity was initially used, manufacturing companies would run their own electrical power plants but as a common power grid became more reliable manufactures eventually

decided to move to the common power grid and so they could go back to focusing on their core business of building products. We are approaching that tipping point in the next few years with corporate networks and cloud computing. As the cost, security, and reliability continue to increase it will become standard to get rid of the distraction and outsource to the cloud. Use of the cloud still needs strong corporate governance and for some organizations (finance, military, Intelligence Community) it will never be an acceptable risk but for many it will. There are security advantages and disadvantages to hosting data in a cloud or outsourcing computing resources, but it is important to remember that the threat will target the place that it can gain the most from. Botnet builders love the idea of consolidating resources into one target. Compromising one cloud provider would give them an instant army. The Advanced Persistent Threat today has to break into multiple systems to find the information they are after; they also would love one target that has all the answers they are looking for.

A couple of technical trends cybersecurity needs to watch are biometric and nanotechnology. The trend toward biometrics is going to lead to new threats as their use grows. First, there are no governing statutes protecting our biometric data today. Second, biometrics are not a silver bullet—the threat will eventually find ways to compromise it. Finally, as we field these systems we will need to build analytics and security integrated into the design. If we use biometrics (perhaps to avoid someone voting multiple times or registering for government aid under multiple names), we need to ensure it has been reviewed by folks who can think like malicious hackers instead of engineers who think about how to make things work. The second is nanotechnology, where generally devices are sized from 1 to 100 nm. These devices can swarm to accomplish more complex tasks. The concerns revolve around building security into the devices upfront and losing control of the devices as they morph into new capabilities.

The legal landscape for cyber is moving in two parallel directions today. First is the idea that private lawsuits will drive public law. The second is that Congress will enact laws to protect aspects of national critical infrastructure, privacy, and intellectual property [22]. There are a number of lawsuits and legislative initiatives ongoing today and there is no clear trend on what guiding principles will come from them. At the same time there are commercial companies offering cyber services to support the military and Law Enforcement Agencies to the point many organizations are outsourcing what was traditionally thought of as government employee-only work because of the lack of skills within the military. At the end of the day this is an international issue. Because the United States and China have developed technological capabilities in the cyber arena, the nations must work together to avoid misperception that could lead to a crisis, according to Defense Secretary Leon E. Panetta [23].

Finally, public perception is that cyber is becoming ubiquitous. We see military strategy books like *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century* by Andrew Krepinevich which states "A terrorist war on the global economy, by means of attacking infrastructure and logistics chains, and through sophisticated cyber-attacks" as one of the scenarios. Twenty years ago Tom Clancy had his hero Jack Ryan stealing a submarine, today in his book *Threat Vector*, Jack Ryan is dealing with cyber-attacks. You see aspects of cyber talked about in the news and debated by politicians. That said the topic is so complex most of the public will tell you they have heard/read about cyber but they will not be able to tell you what it is.

TRENDS DRIVING WHERE WE WILL GO

We are on the brink of a new type of world—a virtual one. We talk about the cyber domain but we generally just mean the network devices. There is a growing part of the digital native generation that is living part of their life inside the grid. They have avatars that represent them in gaming environments like World of Warcraft, there are people who make a living running businesses in virtual worlds like Second Life and World of Warcraft, and we have technology driving us to devices that will provide us with augmented reality allowing us to overlay the virtual over the real world. Some of these virtual worlds are large enough and have big enough economies to be ranked against countries. This presents a new place to have a small "w" war—be it economic or political.

As we look at the leadership of most organizations today there is what we call the "wristwatch syndrome." Most of the people making decisions today were not raised around computers and think of them as support devices—not as the primary means of accomplishing the mission. They still wear their watch even though they have the time available on their cell phone because they have always worn a watch and do not need to change. The younger generation has never worn a watch and many have never had a camera that used film or know how to use a paper map. In fact as we mentioned in Chapter 3 one of the authors was at a simulation exercise and asked a young airman what they would do if they lost the network in the command center and was told, "We couldn't fly anymore." For the generation of military personal who used grease pencils to track movement of entire divisions this attitude was unthinkable. So for the baby boomers who are in charge today they many times do not think in terms of risk to mission when talking about the network. When the digital native generation takes over leadership of the terror groups plotting to attack the west they will default to remote attacks trying to use our mission control systems and critical infrastructure to be the central point of attack rather than a supporting function. This lack of understanding by many of the current national level leaders has led to lack of decisive action. As we look at the near term trends, indecision seems to be a key concern; it could (should) put the countries and militaries at a disadvantage. Nation states and their militaries need to rank the issues facing their country and execute an action plan to address those they can, as well as develop contingency plans to deal with those they cannot afford to solve now.

Some say the problem is too big to solve because of how the internet works. An interesting insight is to look back in history and see we have faced similar problems in the past. Dale Meyerrose, Vice President & General Manager Cyber Integrated Solutions, Harris Corporation, told an interesting story at the 4th annual Homeland Security Conference.

> September 2, 1752 was Calendar Adjustment Day in Britain and the Colonies, correcting the Julian calendar which had gotten seriously out of whack. The day after Wednesday, September 2, was proclaimed to become Thursday, September 14, 1752. This caused some riots among people demanding the return of the 11 days they were cheated out of. The adjustment also moved New Year's Day to January 1 (formerly March 25), and resulted in there only being 282 days in 1751. Thomas Jefferson had his tombstone engraved with two dates for his birth (both Old Style and New Style) and left instructions that two more dates for his death were to be chiseled in [24].

Today this seems odd that folks would get that upset about a calendar change but it took a lot of political will to fix an issue that was growing out of control. The question for us today is will we act on the issues facing us or muddle along?

We have heard the term "Sputnik moment" [25] (when the USSR launched a satellite and the U.S. realized they were behind in the race to space) on the political stage lately. One of the institutions that came out of America's reaction to "losing the race to space" was Defense Advanced Research Projects Agency (DARPA) [26]. DARPA has a cyber thrust designed to enable military systems and infrastructure to operate effectively in the presence of cyber attacks. Technologies that eliminate entire classes of vulnerabilities, that adapt immediately to evolutions or novel developments of the cyber threat, and that raise the cost of employing cyber technologies against U.S. forces are the focus of this thrust. DHS has a National Initiative for Cybersecurity Education (NICE) program consisting of Highlights National Initiative for Cybersecurity Careers and Studies (NICCS) and the National Cybersecurity Workforce Framework. That said we need to look at our open education system—it is a national strength but also presents a threat vector. We do not teach other countries how to build atomic-bombs in our universities, but we do teach them everything we know about cyberspace. Most products related to cyber are not actively controlled by International Traffic in Arms Regulations (ITAR) as we do not have clear rules about what constitutes an export of a cyber capability that can be used as a weapon (classic example here is encryption which is covered by ITAR). As the government (to include the military) has moved from driving technology to buying it, they are now using standard commercial-off-the-shelf products many of which were programmed and built all around the world. Much of the research is now also being done overseas. So as we continue to realize and talk about how critical the cyber domain is to our national interests and what a central role it will play in any kind of conflict we are aggressively exporting everything about it.

The final driving concern is the Cyber Arms Race that is starting. With more and more countries becoming dependent on the Internet it becomes more dangerous for weapons of mass disruption to be built. The chance of a cyber war escalating into a traditional armed conflict is too high to risk; we need to establish rules and processes to ensure appropriate reactions.

There is no quick fix for the many issues we face that need to be addressed at the national level. We need to start making incremental steps on each issue starting with our allies and economic partners. There needs to be a national plan that lays out how we will engage a Computer Emergency Readiness Team (CERT), Law Enforcement Agency (LEA), Legal System and Military, and has incentives and punitive measures built in. It needs senior leadership sponsors and technical competence teamed together.

Finally, it is key to establish the roles and responsibilities for cyber conflicts. If this is a war then it belongs to the military, if it is espionage it belongs to the intelligence agencies, if it is a national security issue it belongs to Department of Homeland Security (DHS). "This is a turf war, The Constitution doesn't allow for idiocy. You either make DHS do their job or you find another way." said James Cartwright, the retired US Marine Corps general who stepped down as vice chairman of the Joint Chiefs of Staff in August and is now with the Center for Strategic and International Studies. The practice of DoD, in the form of US Cyber Command (CYBERCOM) or Northern Command (NORTHCOM), assisting when it comes to attacks against private entities runs into potential legal problems, said Dale Meyerrose, former associate Director of National Intelligence and founder of the Meyerrose Group. "It's against the law for the military to directly support commercial companies," he said. "We sometimes forget that the United States military does not protect the United States except in a very gross aggregate sense. The United States military does not operate within the borders of the United States. What people are calling for is a redefinition of that role [27]."

SUMMARY

So as we look at the ages—Stone Age, Bronze Age, Iron Age, Agricultural Age, Industrial Age, Information Age, Space Age, and now Digital Age—it is clear that technology has been a large driver in our progress. The pace of change has increased over time and continues to accelerate almost exponentially. The domains of war have gone from kinetic to analog to digital and are now enmeshed with our baseline society infrastructure. There are Evolutionary (WikiLeaks, Stuxnet) versus Revolutionary (social media) challenges coming and we need to have a process to address them at the speed of need.

One of the key aspects we have looked at is what a "cyber war" is. The Chatham House Report "On Cyber Warfare" said that, in order to understand whether a hostile action in cyberspace is warlike, it is necessary not just to observe the event but also to understand the actor's intent. Warfare, in the Clausewitzian view, is "an act of force to compel our enemy to do our will." It follows that the actor's intent or "will," on either side of the conflict, must be established before it can be stated that what is taking place is an act of war, or is something else altogether [28]. This traditional view is no longer practical; we cannot identify the intent of someone who steals national security secrets today. Others want to restrict the term to a Congressionally declared war. Again this is not practical today both because it is hard to see a situation where we will be in a declared "War" in the twenty-first century and the term "war" has been co-opted by slogans like "war on drugs." The answer lies not so much in what we call it but what tools we use to address it. We think we must accept the term since it is widely in use and "cyber warfare" is the standard bearer for the cyber conflict challenges we are facing daily. The key is determining and defining what tools do we use to address it: Research, Law Enforcement Agencies, Homeland Security Department, Cyber Command, National Security Agency, and Legislation all have a part but none of them are in charge today.

We must pull from adjacent disciplines such as cultural experts like Toffler (three key drivers of change that are powerfully shaping the future of businesses and governments are innovation, sustainability, and adaptability) [29] and change management experts like Dr. John Kotter (studies have proven that 70% of all major change efforts in organizations fail) [30] to help us organize the right answer. As we move forward into the cyber domain of warfare there will continue to be national and international issues around doctrine, legal principals and generally accepted use of cyberspace as a battle space. For now, regardless of what we call it, there are active cyber conflicts across the national elements of power and continued need for skilled practitioners and capabilities to deal with them.

References

[1] Taleb N. NY Times first chapters, http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html; 2007.
[2] Taleb N. Ten principles for a black swan-proof world, http://www.fooledbyrandomness.com/tenprinciples.pdf; 2009.
[3] Defense Science Board Reports – Capability Surprise VI and VII, http://www.acq.osd.mil/dsb/reports2000s.htm; 2008.
[4] WG CDR Chris Mills, AM. PAK-FA, F-35, F-22 and "Capability Surprise", http://www.ausairpower.net/APA-NOTAM-230210-1.html; 2010.

[5] Joseph Farah's G2 Bulletin. U.S. failed to detect Chinese stealth fighter, http://www.wnd.com/index.php?fa=PAGE.view&pageId=252165; 2011.
[6] Taleb N. NY Times first chapters [online], http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html; 2007.
[7] Didier Sornette Dragon-Kings, Black Swans and the Prediction of Crises [online], http://www.uvm.edu/pDoDds/files/papers/others/2009/sornette2009a.pdf; 2009.
[8] Reed TC. At the abyss: an insider's history of the cold war. New York: Ballantine; 2005.
[9] Davis J. Hackers take down the most wired country in Europe [online], http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all; 2007.
[10] Jackson W. The cyberattack that awakened the Pentagon [online], http://gcn.com/articles/2010/08/25/DoD-cyberdefense-strategy-082510.aspx; 2010.
[11] Krebs B. Russian Hacker Forums Fueled Georgia Cyber Attacks [online], http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html; 2008.
[12] Zetter K. Google Hack attack was ultra sophisticated, new details show [online], http://www.wired.com/threatlevel/2010/01/operation-aurora/; 2010.
[13] Zetter K. How digital detectives deciphered Stuxnet, the most menacing malware in History [online], http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-Stuxnet/; 2011.
[14] Interview with James Gosler Sandia Fellow; May 26, 2012.
[15] McAfee in the crossfire-critical infrastructure in the age of cyber war [online], http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf; 2010.
[16] McMonnell M. Washington post. Outlook & opinions, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.htm; 20l0.
[17] Schneier B. Threat of "Cyberwar" has been hugely hyped. CNN, http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/; 2010.
[18] Interview with Raduege H. January 25, 2011.
[19] Zetter K. Google hack attack was ultra sophisticated, new details show. Wired, http://www.wired.com/threatlevel/2010/01/operation-aurora/; 2010.
[20] Carr J. Dragons, tigers, pearls, and yellowcake: 4 Stuxnet targeting scenarios, http://blogs.forbes.com/firewall/2010/11/22/dragons-tigers-pearls-and-yellowcake-4-Stuxnet-targeting-scenarios/; 2010.
[21] Calabresi M. WikiLeaks' war on secrecy: truth's consequences. Times, http://www.time.com/time/world/article/0,8599,2034276,00.html; 2010.
[22] Interview with Douglas DePeppe Principal at i2IS Cyberspace, Solutions June 1, 2012.
[23] Cheryl Pellerin US, China Must Work Together on Cyber, Panetta Says [online], http://www.defense.gov/news/newsarticle.aspx?id=116235; 2012.
[24] Meyerrose D. GM of cyber integrated solutions. In: Presentation at 4th annual homeland security conference: s.n.; 2010.
[25] Wilson S. What's a 'Sputnik moment'? washingtonpost.com, http://voices.washingtonpost.com/44/2011/01/whats-a-sputnik-moment.html; 2011.
[26] DARPA History. http://www.darpa.mil/history.html; 2011 [accessed 17.01.11].
[27] Fryer-Biggs Z. Debate slows new US cyber rules [online], http://www.defensenews.com/article/20120507/DEFREG02/305070004/Debate-Slows-New-U-S-Cyber-Rules; 2012.
[28] Cornish P, David L. Dave clemente and claire yorke. On cyber warfare. A chatham house report, www.chathamhouse.org.uk; 2010.
[29] Associates T. Technology and innovation 2025, http://www.toffler.com/our-thinking/other-publications.html; 2010 [accessed 17.01.10].
[30] Kotter Dr J. The 8 step process, http://www.kotterinternational.com/KotterPrinciples/ChangeSteps.aspx; 2011 [accessed 17.01.11].