# CYBER ENDEAVOUR 2016

JUNE 21 – 23, 2016

MONTEREY, CALIFORNIA

## "THE INTERNET OF EVERYTHING AND THE IMPACT ON NATIONAL SECURITY"

## (REVISED DRAFT)

### SPONSORS

DOD INFORMATION OPERATIONS CENTER *for* RESEARCH

DEFENSE INNOVATION UNIT EXPERIMENTAL

335TH SIGNAL COMMAND (THEATER)

# EXECUTIVE SUMMARY

The Cyber Endeavour 2016 Report is provided on behalf of the Department of Defense Information Operations Center for Research (DoD IOCR) located at the Naval Postgraduate School (NPS), the Defense Innovation Unit Experimental (DIUx), and the 335th Signal Command (Theater). This report provides an executive summary with major takeaways from presentations and remarks provided by our distinguished and special guest speakers, panel members, and participants, as well as a detailed synthesis of their remarks. This report is not a polished conference report. With only minor editing, the language and grammar used by the presenters, panelists, and attendees is represented within this report as an attempt to capture the authenticity and tone of what was presented and discussed.

**Cyber Endeavour 2016** is the fifth conference in a continuing annual conference series, and was approved by the Office of the Undersecretary of Defense for Policy. The conference was attended by an estimated one hundred seventy (170) participants, panel members, and distinguished and special guest speakers from within the Department of Defense, Federal Government, Industry and Academia. Cyber Endeavour 2016, as with previous conferences, was held in parallel with **Cyber X-Games**, a training venue for Army Reserve Cyber Operations Group (ARCOG) operators to use realistic scenarios for practicing defending and attacking military cyber networks.

The Cyber Endeavour 2016 theme was **The Internet of Everything and the Impact on National Security**, with a separate day set aside each of the following three threads:

- June 21 – **Cyber and Smart Cities**
- June 22 – **Evolving Threats and Challenges**
- June 23 – **Considerations for Operating in Smart Cities**

## THE INTERNET OF EVERYTHING

There were different definitions and viewpoints regarding the Internet of Everything (IoE), but there was general consensus that IoE is really all about the digitization and intelligent connection of people, process, data, and things. Within IoE, things are those key enablers (e.g., systems, devices, sensors, and actuators) that are becoming increasingly dependent on this digital architecture that brings this all together into a cohesive whole, and which also includes other enablers such as cloud, mobile, security, big data, and analytics that comes with it.

## IMPACT ON NATIONAL SECURITY

There was general consensus that IoE is one of the most significant disrupters in our information age (and information-enabled industrial age), and that it changes the political, military, economic and social dynamics between the U.S. (and its allies) and its adversaries (state and non-state actors). There are many benefits to be gained from embracing IoE in the U.S., but in doing so we are now increasing the threats to our critical infrastructure (unsecured) and national security from hostile states, terrorists, non-state actors, and internal actors who are rapidly operationalizing and weaponizing these capabilities, and who have and will continue to use these to the detriment of our nation.

## KEY TAKEAWAYS

- We live in an increasingly urbanized world. An estimated 54% of the world's population currently lives in urban areas, and that is projected to increase to 66% by 2050.

- The most rapid growth in large cities (mega-cities) is occurring in the poorest and least developed nations, those countries who are least able to handle the political, social, economic and environmental implications and problems associated with rapid urbanization.

- Coincident with this growth is the rise and evolution in Cyber and Smart Cities, cities that leverage integrated people, processes, and technologies to make near real time decisions to successfully achieve its objectives. They offer a promise of doing things more smartly though optimizing existing facets of the city at its core, and in doing things more effectively and efficiently.

- There are many challenges in living or operating in Cyber and Smart Cities, to include security and policy, our ability to make sense of all the data, our willingness to automate everything without understanding the risks, and our increased dependency on areas that are outside our control or view.

- We need to stop overselling/overhyping cybersecurity. There are no walls strong enough to protect our Cyber and Smart Cities (e.g., a cyber version of circumvallation), critical infrastructures, and IoE. However, we can make them more resilient and harder for the adversary to attack.

- We cannot have 100% privacy and 100% security, so we need to find the proper balance. We also need to find a proper balance between security and generativity (creating something new), the former of which is of little importance to our current generation, and the latter of substantive importance.

- No one operates in a cyber-free environment. Even in countries where only 30% of the population have access to electrical power, close to 100% have cell phone usage.

- We need to quit telling cyber experts to "do something." Just like anyone else, give them a mission and let them work it out.

- We need to remove the barriers to identifying and publicizing vulnerabilities. Let's find ways to encourage folks to bring these vulnerabilities to the attention of the government (as well as the corporations that had these vulnerabilities). Threatening and jailing and bringing lawsuits against potential patriots and ethical hackers are not working out too well, and might drive these folks underground.

- Our military institutions demand career breadth, which isn't necessarily attractive to cyber experts who prefer to focus narrowly on their field of expertise.

- Our military and government institutions should start embracing folks who are unorthodox or unembraceable, and find a way to bring them into their cyber forces. We have done this throughout history, especially WWII, why not now? These may be the exact folks with the right skill sets we need, and we do need to acknowledge the fact that we cannot train and maintain enough cyber forces by going the conventional route.

- We are rapidly automating planes, trains, automobiles, and swarms, even robotic jellyfish, each of which operate in cyberspace. Securing and protecting these systems is critical. We cannot forget the second and third order effects of autonomy.

- We'll never have enough people to get out of 'this;' automate more and reduce dependence upon people and human error.

- Everyone wants to do offense, but don't forget defense – you don't need permission to do defense.

- There is international law but no approved definition for sovereignty in cyberspace. Some claim cyberspace is outside the reach of the sovereignty of the state. Others believe that there is cyber sovereignty when there is a physical (cyber) presence in the territory of another state, remote physical destruction if injury, remote loss of functionality, and/or usurpation of inherent government functions (e.g., the use of cyber activities to influence election results).

- There is some philosophical debate on cyber warfare and sovereignty from a Just War theory perspective, which has as its lynchpin civilians' immunity from harm. In cyber warfare, can harm be aggregated to the point justifying a nation to respond with a violent, legal response? For non-consequentialists, the answer is likely no; for consequentialists, the answer could well be yes.

- While the U.S. might want to conducts its cyber operations according to international norms and laws, our adversaries don't play that game. Therefore, deterrence is a must, and needs to be a key element of our cyber strategy and planning (it also says so in the DoD Cyber Strategy). Our government and military institutions should consider identifying those activities that are unacceptable to the U.S. and its national security, then make those activities illegal, and then signal to the rest of the international community that we will not tolerate those activities. We then need to take action if the adversary conducts those activities. If we do not, we will simply become suicide victims of international law.

- Freedom of expression, the right to privacy and to be forgotten, and cyber sovereignty is obviously going to be seen around the world through different lenses. There are even differences between the U.S. and its allies, bringing challenges from a legal/constitutional perspective on how to put these into doctrine, policy and plans.

- We have a lot of smart partners (other nations). We don’t need to replicate capabilities that we can share with our partners.

- Public private partnerships are a must if we are to successfully engage the enemy and win.

- Treating partners with respect brings great results, as witnessed between the U.S. and Canada on cybersecurity and grid cooperation and information sharing (we share our electric grid with Canada and parts of Mexico).

# DAY ONE – JUNE 21, 2016

## THE INTERNET OF EVERYTHING AND THE IMPACT ON NATIONAL SECURITY – CYBER AND SMART CITIES

## SETTING THE STAGE

*Dr. Hy Rothstein, Director, DoD IO Center for Research at the Naval Postgraduate School*
*Dr. John Arquilla, Chair, Department of Defense Analysis, Naval Postgraduate School*

Our first two special guest speakers set the stage for the conference, providing their perspectives on the rapid urbanization of the world and the rise of smart cities, some associated national security considerations, and challenges and solutions associated for protecting and securing our cities and smart cities from a historical perspective.

### Rapid Urbanization of the World

Based on current demographic statistics, an estimated 54% of the world's population now lives in urban areas, and that proportion is scheduled to increase to 66% by 2050. Today, the most rapid growth in large (mega) cities is occurring in the poorest and least developed nations, those countries who are least able to handle the political, social, economic and environmental implications and problems associated with rapid urbanization.

### Rise of Smart Cities

The world is also experiencing a rise and evolution in "Smart Cities," where innovations and technologies are creating great opportunities but also posing challenges to our security. Humans are already interconnected via smart phones and devices, and there are innumerable smart energy meters, security devices, and appliances already being used in many cities. Homes, cars, public venues, and other social systems are on the path of full connectivity. Intelligent transportation will access the internet that connect transportation to GPS signals and locations, weather data, and traffic updates, and these integrated systems will contribute to public safety. Protecting the systems that gather data and trigger emergency responses will be both technological and security challenges that need to be fully addressed.

### National Security Considerations

There is a definitive overlap in the growth of these smart cities and the rapid megacity growth in the poorest developing countries. Protecting our own smart cities is challenging, but relatively straight forward. There will be many challenges and a lot of "fog" for the Department of Defense when operating in densely populated smart cities overseas, as the Department of Defense cannot bypass 70% of the world's population or ignore an increasingly urbanized domain that offers haven to terrorists and non-state actors that are posing an increased threat to our national security.  It appears the U.S. Army and Marines have been putting a lot of thought into operating in these mega cyber cities, as have the Cyber Community in talking about threats and challenges and opportunities and intelligence requirements associated for operating in this urban terrains. However, an area that needs to be improved is increasing the communiques and interactions between the ground components (U.S. Army and Marines) and the Cyber experts who ultimately have to support and facilitate ground operations.

**Protecting and Securing our Cities (and Smart Cities) – Historical Perspective**

Throughout history, protecting cities has always been a challenge.  It took on new challenges with the rise of aircraft and strategic bombing a century ago, and recently taken on a new dimension in the wake of terrorism as a form of war.  Think of Mumbai in 2008, when ten gunmen carried out a series of twelve coordinated shooting and bombing attacks lasting for four days, or the numerous gun swarms in various cities around the world.  These are becoming more a norm than the exception.  With the increasing cyber threat from state and non-state actors, we need to think about the increasing cyber threat to cities.

Throughout history, cities have represented the highest level of advance in civilization, and have persisted as a focus of technological advance, settlement, loyalty and commerce. Everything we do has centered around cities, and the protection of these cities with walls, or circumvallation, has been both a strategic and tactical imperative throughout history.  Jericho, the oldest continuously settled city in the world, had twenty different walls throughout its existence.  Constantinople built three walls that served fairly well. The city in fact was all that remained of the Byzantine Empire at various points, but it outlasted Rome for over 1,000 years.  The construction of walls around cities does not necessarily guarantee the security, and oftentimes the free flow of information and interaction with others provide for a better and more proactive defense, such as with Athens.  However, even the strongest walls do not mean that a city or fortress is impregnable, as was the case with Tobruk during World War II that withstood a German and Italian siege for eight months.  Its walls were virtually impregnable to air and artillery attack, but in June 1942 the city fell in a single day and 33,000 Allied prisoners were taken.  The same was true during the Battle of Singapore in February 1942, when Japan invaded and quickly captured this "British Stronghold," along with and an estimated 88,000 British and Allied troops with a force 1/3 the size of the Allied troops.

When looking at cities in context of cyberspace and Cyber Cities, there is no such thing as a good (impregnable) firewall.  As a community, we need to be careful about putting our faith in walls, as firewalls are really only good with protecting against things they already know.  As was the case in Tobruk and Singapore, adversaries came up with innovative exploits and new ways of approaching the problem when traditional methods failed.

Some cities throughout history have demonstrated resilience, however, when under strategic attack.  In looking at London during World War II, London demonstrated inordinate resilience to the strategic bombing campaigns by Germany.  Theorists are that time postulated that if a nation's air forces flew over cities and dropped their bombs, the people in that city would panic, and the attacking force would achieve their war objectives without having to fight the battle on the ground.  That was not the case.  The U.S. has to develop the same type of resilience against cyber attacks. The question becomes, "do we have the will and are we in a position today where our people could remain calm during a major cyber attack, or would we panic and have our cities become crippled?"  While London demonstrated extraordinary resilience in the face of strategic (kinetic) attacks, it is going to be harder for our nation, as well as other nations throughout the world, to achieve cyber resiliency in the wake of a deliberate cyber attack (kinetic and non-kinetic) or possibly even to an incidental (Act of God) event. The following examples speak to some of the challenges of attaining cyber resilience:

- In April 2013, several snipers opened fire on the PG&E Metcalf Transmission Substation, severely damaging 17 transformers. Had the snipers struck a few more spots at this substation, power would have been degraded in the Silicon Valley for several months, and the ability to replace damaged equipment would have taken a great amount of time since much of this equipment was specialized and produced in Europe.
- In June 2016, Kenya experienced a nationwide blackout when a small (Vervet) monkey fell on a transformer of the Gitaru Power Station and tripped it, which caused other machines at the power station to trip on overload.
- In December 2015, suspected Russian hackers conducted a cyber attack on the Ukrainian Power Grid in Ivano-Frankivsk by taking administrative control of its power grid that quickly shut down the entire city of 250,000 people. The good news was that the technology was a little older and was capable of being manually operated. So working manually, operators were able to throw switches and used manual dials, and were able to get the city back up within a day. They were saved by the fact that their personnel could operate these systems.

However, in most U.S. cities with automated systems, there is no ability to run them manually. When we think about our military, the preponderance of these systems are fully automated. Our military forces are no longer trained to operate and reconstruct them if damaged or destroyed. In the middle of a future campaign, the time consumed in getting these complex, automated systems back online would have a profound effect and increases the likelihood for the loss of life.

When looking at the technological development of cities over past two decades, there is a level of vulnerability that dwarfs the perils that our forces face today in the field, in the air, and sea. It is almost unimaginable to think about the degree to which our vulnerability has opened up. Part of the story is about modernity while the other part is that much of our infrastructure predates the Internet. As an engineering problem, we are taking old technology that is not designed for information security and increasing connecting it to the Internet. This creates problems at both ends. On one end, most advanced technologies that are disruptive are hard to substitute, replace or repair. On the other end, we have an antiquated infrastructure that is still hard to replace but is connected in ways that make them increasingly vulnerable. These are two ends of a complex, difficult problem, and opens up the possibilities that cities will become the target of strategic attack.

Our adversaries (state and non-state actors) are not only conducting cyber intrusions into our defense systems, but also into commercial systems. While many of these intrusions are undertaken for stealing information, others are conducted in order to map systems enabling information preparation of the battlefield and learning how to make attacks possible. There is not the appropriate level of concern, or sense of urgency, on this problem since we have not had a Digital Pearl Harbor. This might not be the analogy to consider, and Pearl Harbor was a location where most of the American power and infrastructure was located in the Pacific Theater. A better analogy might be “Harbor Lights” that occurred in the early days of World War II, when the waters along the Eastern Seaboard were teeming with German U-boats who used our well-lit coasts to target and blow up our ships. Our coastal cities at first did not want to turn off the lights at night figuring the economic costs would be great, and thus the entire seaboard remained illuminated which resulted in our merchant ships remaining highlighted and easy targets. Things got better when President Roosevelt bent to pressure and ordered blackouts, as well as the fact that the Navy changed its tactics from sending destroyers out to chase submarines and instead started escorting convoys.

In cities throughout the world, and especially our mega cities, those lights are on and they are highly illuminated. These cities are increasingly becoming a rich and appetizing target set to nation states, state and non-state actors, and rogue warriors who have already and will continuously strike anonymously.

The world and our nation have numerous challenges to address when considering how to protect our cities and underlying "cyber infrastructure." Within the U.S. alone, there are over 3,000 companies (power providers) providing power throughout our nation. While many of these power companies have similar power systems and devices, and are increasingly becoming connected to the Internet, each has a different security structure. The weakest link thus allows a portal into that national power and information sharing infrastructure. Additionally, within the U.S., there are over 50,000 Supervisory Control and Data Acquisition (SCADA) systems that are currently unprotected. Identifying these SCADA systems is a relatively easy task with the advent of Shodan, a search engine that enables a user to find specific types of computers and devices connected to the Internet. Our nation also has to think about the physical threat to cyber infrastructure, such as the Metcalf sniper attack. This includes pulse or high energy weaponry and conventional explosives in the right spot, such as downtown Manhattan/Wall Street, both of which would create significant damage. As a nation we need to increasingly apply our inventive energy in looking at this remarkable target set, using our laboratories and other institutions for testing new methods and tools, and then taking them to prime time.

In postulating as to where in the world would a high intensity war employing coordinated conventional and cyber warfare occur, we could look to North Korea and the Korean Peninsula. The Demilitarized Zone (DMZ) is an extremely narrow strip surrounded by the most concentrated military presence in the world, to include a substantive U.S. military presence. North Korea has a large contingent of "Special Forces," an estimated 100,000 troops. They have weapons of mass destruction (nuclear, biological and chemical) as well as a sharp cyber capability. North Korea's Mirim College has an elite hacking program that has been churning out 100's of cyber warriors each year over the past two decades. North Korean's cyber prowess was evident when their government employed a fairly sophistic cyber attack/hack on Sony Pictures Entertainment (according to FBI findings). A full scale war on the Korean Peninsula would entail one of the most concentrated cyber targets on the planet based on interdependent power and infrastructure. One could imagine a coordinated cyber attack hand in hand with a physical attack, which has not been seen other than in prototype in 2008 when Russia invaded the Republic of Georgia. When talking about areas of dense populations, Korean Peninsula cities and their civilian population would be particularly vulnerable, especially those in the Republic of Korea (ROK). These urban areas/cities would be plunged into darkness and chaos for weeks or months. This would place military affairs (conventional and cyber) at the junction of urbanized society, and signify a true transformation of future conflict. It would be tough for the U.S., ROK, and Allies to stay calm.

Within the U.S., our national security must be thought in terms of the increasingly urbanized world, but also about the security of the individual as well. During the 18th century, individuals with a frontier spirit and ethic of self-protection considered themselves responsible for their security, supported by small groups of soldiers and rangers/militia. They provided their own self-defense, and settled many of their own wars. Today, cybersecurity is considered a function of the government for the people who sell them powerful and attractive devices that may or may not contribute to our nation's overall security and protection. Individuals have come to believe that others are now responsible for their security. What is needed is finding a balance between the government and individual, and ways to recapture that part of the frontier spirit. Cyberspace is a vast virtual wilderness that grows in complexity and size and beauty, but also carries its dangers. A challenge for our nation's leaders is how we deal with the individuals' mindsets that others are responsible for their security, address the many cyber vulnerabilities of our cities, and an increasing potential for individuals (and their cyber systems) to have an unwitting role in the attacks that may occur.  While we need to worry about infrastructure, connectivity, and functionality of our nation and smart/cyber cities, we must also be attentive to needs of the individual as the people are the city.  That is a security problem that challenges all of us to have our best day.

We live in an urbanized and increasingly urbanizing world. We live in a time when the latest technology is now increasing its threat capability at a time when the target set is broader.  It is a confluence of factors that creates for massive insecurity. It is our challenge to identity and detect, and disrupt those who would attack us. It is a time when above all else, we need to keep calm and to carry on.

# The Internet of Everything Current and Future

*Mr. Joseph Beel, Strategic Programs Manager, CISCO*
*Mr. Stephen Orr, Distinguished Engineer, CISCO*
*Dr. Steven Chan, Director, PACOM Sensemaking Fellowship*

During this panel, panel members and participants characterized and defined the IoE and highlighted some current IoE cyber threats and cyber vulnerabilities.

**The Internet of Everything – The Perfect Storm**

The Internet of Everything (IoE) is the digitization and bringing together of people, process, data and things. Within IoE, things are key enablers (systems, devices, sensors, actuators, etc.) that are becoming increasingly dependent on this digital architecture that brings this all to fruition, which includes other enablers such as cloud, mobile, security, big data and analytics that comes with it.

The IoE is like a "perfect storm" that has multiple concurrent inflection points to include:

- Internet Protocol (IP) becoming the standard communications protocol across many, if not all, industries and sectors in the business and military world,
- Cloud computing which is becoming rapidly available to everyone,
- Edge or fog computing that gets incredible power into the devices at the edge (you can run a server as a module of a router),
- Software applications (software applications are epitomized on smart phones, which enables them to have incredible computing capability and 24x7x365 connectivity and access to data/information),
- Big data and analytics, and
- Miniaturization of sensors and actuators becoming cheaper and increasingly connected to the Internet.

Within this perfect storm, the greater the machine to machine, machine to people, and people to people communications and connections, the more rapid the growth in the utility of what you are doing within your organization with IoE. As more and more things converge on the network, an organization needs to bring in the management, simplicity, and analytics to control this as well. Within any business or organization adopting IoE, there is a need to first establish a solid foundational approach to connectivity and security. If you do not build security in at the beginning, it is going to be very difficult to architect security back into it. Some additional foundational elements that are built on connectivity and security include the software and analytics driving towards the desired effects, applications and solutions, platforms, and the actual business and mission outcomes you want to accomplish. An architecture of connectivity and security needs to be in place in order to achieve business and mission outcomes without putting yourself at risk.

Phone systems were one of the first "things" to converge into IP. This was followed by devices and systems that included video systems, access control networks and devices for buildings, and lighting (which is increasingly becoming as service of the network). We can eliminate electrical wiring to lighting fixtures, and LED reduces

65% of the electricity costs. With LED, you don’t have to run electrical cable to every light which reduces weight, and LED can be used in sensors or security measures. Imagine changing your security or warfighting posture by changing colors to let people know, and LED can be useful in dangerous environments.

There are different lines of business that have a significant impact with the IOE, most if not all of which come back to the defense sector as well. These include:

- Connected factories, such as factory automation with robotics, factory wireless, and factory security,
- Connected utilities and substations (utility monitoring and control)
- Connected oil and gas in austere environments (there are mining companies employing IoE that have increased safety, decreased costs, and exponential growth in productivity)
- Smart and connected cities
- Connected sports and entertainment, such as stadium Wi-Fi and video/facial recognition capabilities that are so good in the stadium that they are increasingly being used by security and law enforcement entities around the world to help identify and arrest the world’s most wanted criminals
- Connected transportation, such as connected rail and roadways (also helped Paris solve its massive parking problems)
- Connected public safety, a good area where you can bring things to edge such as body worn cameras and fully connected police cars (such as in Dubai, where they are fully connected with a router running in trunk of the car).

Barcelona is seen by many to be one of the most connected, smart cities in the world. Barcelona’s local government and smart city planners believe that openness with its citizens, stakeholders, and utilities is the best way to achieve their goals (revenue, citizen experiences, jobs, productivity, and cost avoidance). Within Barcelona’s smart city architecture is smart lighting, smart buses and bus stops, smart parking, smart waste, smart buildings, smart water, connected learning, and most importantly, smart citizens. As a result, Barcelona’s smart city initiatives have creating $3 billion in value.

In context of “the people are the city,” you can get a lot out of your people if you are working hard to make them smarter and keep them happy, and IoE is seen as an enabler by many countries and cities (such as Barcelona). Dubai also prides itself on making its citizens happy, and has embraced IoE. There are also self-enlightened organizations such as Southwest Airlines, whose leadership advocates that no employee will ever treat a customer any better than the company has treated them.

Within an IoE environment, it is the pervasive connectivity of people, processes, data and things that create opportunities for enhanced efficiency, effectiveness and productivity, and all of which translate to the Department of Defense.

**The Internet of Everything – Cyber Threats**

Most cyber professionals or hackers, within minutes of logging online and having the right equipment and applications, can access most any organization’s network to obtain information on the services that network provides, who is on the network at that given time, what applications and devices/systems one has at home, and how to access and/or exploit the systems and devices one uses at home. The increasing number of personnel using devices such as Apple remote desktops, iPhones and other smart phones/devices, and SSH/FTP in their day to day routines. By doing so, these personnel are creating new threat vectors that are continuously being advertised by their devices, which in turn makes them more susceptible to both outsider and insider attack. Most people don't realize this is happening and the extent to which their actions and systems that are ubiquitously connected to the Internet are creating new threat vectors.

Once the cyber professional and hacker gets onto a network, they can obtain invaluable information even if encryption is employed. An example of this is Wi-Fi encryption between user and access points. Most people do not realize that multi-cast traffic on a Wi-Fi network is shared and not secure. Each user has the same group encryption on that Wi-Fi network. As a result, if someone is on a secure network, at a minimum the services that are being advertised and devices being used by you are out there in the open. Additionally, it is readily easy for the cyber professional and hacker to decrypt your multi-cast traffic. Another culprit to be aware of is Bluetooth and things that sync with Bluetooth, such as laptop computers, headsets, iPhones, iPads, and other smart devices. The applications to exploit Bluetooth are readily available and free; with these applications a cyber professional and hacker can access all Bluetooth enabled devices and start correlating their respective global identification information which are "globally unique." With Wi-Fi and Bluetooth activated (on condition) on your device(s), anyone with the motive and intent (and access) such as "big box stores" now has the ability to track you. You are also adding, wittingly or not, to your IoT footprint.

As we do more IoT, and as IoT devices get smaller, and as CPUs become increasingly constrained, most users will leave Wi-Fi and Bluetooth on without understanding how much information they are pumping out into the open air that is not encrypted. It will get even worse, as there is a move afoot by the Institute of Electrical and Electronics Engineers (IEEE) to develop standards for Wi-Fi regarding service discovery and service advertisements. Today, one can only discover services by joining the network. In the future, services will be announced that can be picked up before one joins the network. With IoT becoming more pervasive, an infinite number of sensors and devices on the network will be advertising their services based on their name (global ID) and capabilities portfolio.

Even current encryption standards, AES128, have a limited role in securing and protecting our cyber systems, networks and data with the dawn of quantum computing. Instead of having an estimated lifespan of thirty years, current estimates suggest a lifespan of ten years or less, affording an adversary to collect and store this encrypted data and information in warehouses and decipher at a later date (it's a long war). Additionally, encryption for encryption sake is not effective. It is important to first authenticate the device and the user to make sure there is some trust before encrypting. Even if a device is encrypted, an adversary can still create havoc with memory modifications and IOS binaries. In the end, it is important to be confident that the device is what it says it is, is doing what it is supposed to do, and has remained unmodified during its use.

Earlier discussions highlighted the fact that walls are impenetrable, to include firewalls. An adversary is not likely going to attack you head on by attacking your firewall when they can compromise something smaller without the same security features as that of the firewall, or any security features at all. Once an adversary gets access to one of your smart devices, they can access other devices within your IoT footprint, creating new threat vectors and subsequently punching holes in your firewalls. Additionally, an adversary will more likely attack a DNS server (much easier to exploit) rather than those IoT systems, servers, and devices employing IPv6. With more connected devices on the internet, encrypted or not, there will be more data on the network and more things that an adversary can learn upon which to conduct their own “cyber intelligence of the battlefield.”

With the rise of Smart Cities, ensuring that critical infrastructure is secure and trusted is of paramount importance. However, our utility companies have industrial control systems that are highly vulnerable, with energy utilities the most vulnerable as they are the least to invest in security and among the first to connect their unsecured control devices and operational networks to their business networks for increased efficiency and cost savings.

It is important for our nation to build a secure, trusted network, and then make sure the foundation is secure. Only then should we layer on all the applications and IoT capabilities. We need to make sure that the foundation is not compromised, as then everything else you put on it will eventually be compromised. Some recommendations and considerations include:

- Developing a trustworthy system strategy to protect the device, protect the network, protect the application and protect the data.
- Authenticating the device, getting on the network, and encrypting data on the network (device side); authenticating the operating system (OS), having the device authenticate itself to the network, and having the device start encrypting data on the network; and making sure the device is valid, who it says it is, and that it is running a valid OS that has not been compromised.
- Conducting big data analytics with only a trusted device. If you do not trust the device, then it is unlikely that you will trust the data from the device. Further, if the device can be compromised, then data from the device can also be compromised.
- Protecting devices by shipping them with secure unique device identifiers, certificates burned into the device or memory to ensure we know what it is and who it came from.
- Visualizing the trust within networks, out from the sensor/device to the data center and through the enterprise.
- Keeping securing simple, as the more security you layer on the network, the more complex it appears and becomes to operate. Secure by default is being looked into more, and then plugging devices into networks that are automatically secure.
- Ensuring standards bodies upgrade encryption standards and projecting forward.
- Keeping high assurance moving forward.

### The Internet of Everything – Cyber Vulnerabilities and IPP/PPA Double Jeopardy Paradox

There is an interesting demarcation point between IoT and IoE, a concept called “Double Jeopardy.” Within our cyber cities, smarter cities, and smarter mega-cities, we have a plethora of things where we can only see the IP device. Within the electromagnetic spectrum, we will likely see a little further. While we have some limited resolution by being able to see some of the things that are connected, but for the tens of billions of devices that are concentrated within one city, it becomes very interesting. This is where the Double Jeopardy comes into play. This situation is beyond what we can control. In using electric utilities as an example, what happens if someone uses an independent power producer and buys power with power purchase agreements when needed? Business sophistication is very high, but they can see only see the power of the things that they are producing and in control of such as their generators, transmission lines, and distribution. If they are buying from an independent power producer, it is unlikely they will have insights as to their security, resiliency and vulnerability postures.

Most of the megacities are emerging in the Asia-Pacific region, and include Tokyo, Mumbai, Delhi, Shanghai, Jakarta, Manila, Beijing, and Osaka-Kobe. Many things within these megacities center around energy and marquis events.

In looking at the Internet of Everything in a Smart City, the foundational building blocks are strategic infrastructure supporting critical infrastructure (e.g., microgrid, smarter city, and mass transit), both of which are predicated on continuous streaming data.

Within the Asia-Pacific region, there are some interesting aspects of the IoE and megacities.  One potential cyber vulnerability are actually buoys that serve as tsunami warning devices; if they are attacked by an adversary, the power grid is shut down.  Another factor with the Asia-Pacific region involves the substantive utilization of water for the biofuel and coal throughout the region, highlighted by the fact that China and India will account for 70% of the total electricity generated and 21% of the total water consumed due to electricity generation by 2035.

With increased communications requirements in Smart Cities, bandwidth is becoming a bigger issue.  If a utility company were to increase surveillance/monitoring of its sub-stations, then that sub-station will likely not be able to effectively communicate with its central operating system.

From an Internet Communications Technology (ICT) perspective in the Asia-Pacific regions, Japan was ranked 11th, Singapore 19th and Indonesia 108th.  On a side note, Indonesia protested its rankings, especially in light of its ranking in global competitiveness.

From a Global Competitiveness Index (GCI) perspective in the Asia-Pacific regions, and with ranking based on infrastructure, business sophistication, innovation, IPP/PPA, and renewables integration and latency stability, Singapore was ranked 2nd, Japan 11th and Indonesia 34th.  It was interesting to note, however, that Japan and Indonesia have the exact same rankings for each of the five factors.

In looking at total net power generation within Hawaii, electric utility companies produce an estimated 50% of their power, and purchase the other 50% of their energy from independent power producers.  This is similar to many of the countries in the Asia-Pacific region.  Within Japan, the electric utilities are deregulated and federated, with each having their own independent power producers.

So supply chain wise within the U.S and Asia-Pacific, you cannot see too much.  You might have your own cyber policy, but possibly little to no insights in the policies of the independent power producers.

In looking at two of the five factors in the GCI – IPP/PPA and renewable integration and latency stability – there is a consistent upward trend in both IPP and PPA for all countries involved in this research initiative, as well as a corresponding, latent stability of all these systems on a downward trend.

Across the board, if we rank everything from security to resiliency inside cities that are becoming smarter and more mega through both urban sprawl and reverse urban sprawls, and these cities become more connected, this becomes a ‘double jeopardy’ situation.  If solar panels on houses trip offline due to a cyberattack or natural event, not only do these homeowners not contribute to the load that is being sold, homeowners are now drawing from the load. This situation happens in Hawaii, as it does across the Asia-Pacific region.

# CYBER TRAINING – VENUES FOR CYBER CITY TESTING AND TRAINING

*Mr. Peter Christensen, Director, National Cyber Range*
*Major Michael Lewis, S3 Army Reserve Cyber Operations Group*

During this panel, panel members and participants shared their perspectives on the cyber threat in context of automobiles and IoT, DoD approaches and National Cyber Range (NCR) resources to mitigate cyber risks through Cyber Testing and Training, and Army Reserve Cyber Operations Group (ARCOG) Cyber Protection Team (CPT) training.

**Cyber Threats in Context of Automobiles and Internet of Things**

Cyber threats are exploiting exposed vulnerabilities in infrastructure and control systems as we speak. The challenge from a DoD perspective is that we are not eliminating these cyber threats earlier in the acquisition process – this is a systems engineering problem.

Stuxnet changed the way people looked at malware, as malware took a never-before-seen leap from the digital into physical world. The Stuxnet computer worm destroyed numerous centrifuges inside Iran's Natanz uranium enrichment site by targeting (reprogramming) their Programmable Logic Controllers (PLCs). The Stuxnet computer worm also infected other industrial facilities throughout the world like power plants, dams, waste processing systems, and similar operations.

Cyber attacks exploit a system’s resources and its channels, methods, and data items that are involved and need to be understood as part of the “attack surface.” SANS defines attack surface as “a system’s exposure to reachable and exploitable cyber vulnerabilities.” As we move more into IoT, this definition needs to be expanded to include focusing on not the interior of systems boundaries, but also on the exterior to systems boundaries.

In looking at the automobile industry in the past, the attack surface was limited. In recent years, the attack surface has increased on automobiles, as there are now over 100 million software lines of code used by 70,000-100,000 microcontrollers. In 2014, a group of hackers caused a demonstration vehicle to slam on its brakes, and the following year have a vehicle drive off into a ditch. In a recent article on hacking vehicles from the Internet, a Spanish researcher demonstrated the ability to monitor and control float trucks, public bus, or delivery vans via the Internet. The researcher used the Shodan search engine to identify – through their IP addresses –thousands of vehicles that were connected to the Internet via c4max Smartbox Telematics Gateway Unit (TPGU) and modem. The Spanish researcher was able to obtain vehicle speed, position, and other parameters. There was an administrator interface that could be remotely accessed with no user name or password, and the researcher was able to get critical information on some advanced features that changes mission routes. From a tactical perspective, these are some of the things one might do to an adversary’s supply chain.

By 2020, there will be more than 25 billion embedded/intelligent systems, 25 billion applications, 4 billion people, and 50 trillion gigabytes of data connected to IoT. This is a tremendous opportunity. However, what might scare people is the $4 trillion revenue opportunities, in large part due to techno-lust.
It is unwise for people to assume that their systems and technologies have built-in security. Most of the user base are clueless, resulting in more people becoming victims.

From a DoD perspective, DoD is trying to change policy and guidance to drive security earlier in systems engineering and testing activities in order to begin implementing better processes. Guidance and policy will not solve the problem. Additionally, DoD implementation of cyber policy and practice created "technical debt" which is defined as the cost of work that must be completed before a job can be completed resulting from:

- Consequences of flawed requirements, design or implementation (incurred unintentionally)
- Consequences of organizations making a decision to optimize for the present rather than the future (incurred intentionally)

**Department of Defense Approaches and National Cyber Range Resources to Mitigate Risks through Cyber Testing and Training**

The DoD has implemented several cybersecurity policies to help mitigate cyber risks earlier in the process in systems acquisition, as well as provision cyber range resources to provide cybersecurity testing as a service to its customers. Historically, DoD implementation of cybersecurity policy and practice has created technical debt, the results of the consequence of flawed requirements (Type I debt), or by intentionally making the decision for optimizing for the present and not the future (Type II debt). Many folks find this difficult to quantify, but if you look at last year's National Defense Authorization Act and consider the millions of dollars Congress has appropriated for us to evaluate the cybersecurity policy of legacy systems, this translates to the tactical debt we have created because we have not engineered and tested systems early on in the acquisition process. We get techno-lust and throw these systems out there, and then apply some security patches later.

In looking at recent DoD Test and Evaluation (T&E) annual reports, there were 300 different types of vulnerabilities in the 40 programs tested and evaluated. The top three vulnerabilities were programs using out of date software, unpatched software, and/or software with default user names and passwords. These problems should not happen, and these kinds vulnerabilities should not be discovered when the DoD takes systems to Operational Test and Evaluation (OT&E).

From a Cybersecurity perspective, the DoD is trying to use some of these early phases of systems engineering and OT&E to better identify what the cybersecurity requirements are as well as understand and characterize the attack surface. This will help testers guide their testing strategy, and drive processes and activities that includes early security control verification to obtain empirical data to help verify that the baseline technical requirements have been satisfied of these programs. This addresses what we refer to as Type I technical debt. The DoD will then go into the latter phases of testing to reduce Type II technical debt that would then enhance the resiliency of these systems in a relevant cyberspace environment. This testing included cooperative vulnerability assessments to identity and close exposed vulnerabilities, and to highlight adversarial penetrations and its mission impact. This testing goes well beyond a Red Team identifying just how many times they were successful in getting into DoD networks and systems. What should be of greater importance is taking a comprehensive look at the missions that need to be accomplished by that system, critical systems that are involved in supporting that mission, and the critical data exchanges…and then come to understand where we are lacking effective protection measures or where a protection measure is improperly configured.

The DoD is increasingly training its Cyber Mission Forces (CMF) in relevant environments so they can understand how the adversary may try to exploit their systems, what kinds of activities they need to do to close or deflect those attacks left of exploit of possible, or once the adversary is in your system, try to detect, respond, restore and recover.

One of the primary DoD organizations responsible for Cyber Testing and Training is the Under Secretary of Defense for Acquisition, Technology & Logistics (AT&L) Developmental Test and Evaluation (DT&E) office who is responsible for managing the Test Resource Management Center (TRMC) and Cyber Test Ranges.

- TRMC provides Cybersecurity T&E ranges and services that includes end-to-end test support, test bed design support, cyber and testing expertise, threat vector development, customer traffic generation, custom sensor and visualization support, custom data analysis, and integration of custom assets.
- Cyber Test Ranges enable recreating relevant cyberspace environments to evaluate cyber defenses and offenses, and to train warfighters. They provide an opportunity to rehearse tactics techniques and procedures, in an environment where one can rapidly change the assets, operating systems, system configurations, network configurations. It is not just virtual, but instead a combination of virtual and real hardware and software where appropriate.

The NCR was developed by DARPA in 2009-2012, and transitioned to the TRMC in October 2012. TRMC continues to operationalize NCR capabilities for use by DoD Test, Training, and Experimentation communities. The NCR provides secure facilities, technologies, repeatable processes, and a skilled workforce; creates hi-fidelity, mission representative cyberspace environments; and facilitates the integration of Cyber T&E infrastructure through partnerships with key stakeholders across DoD, U.S. Department of Homeland Security (DHS), industry, and academia. The NCR consists of 5 components"

- Computing assets at the Lockheed Martin facility in Orlando, Florida (government owned contract facilities),
- Encapsulation architecture and operational procedures that allows the NCR to segregate computing assets into five distinct, cryptographically isolated, realistic cyberspace ranges,
- Integrated cyber event tool suite that allows NCR to automate the process,
- Secure, remote connectivity across the Joint Information Operations Range (JIOR) and networks, and
- Cyber test team.

IoT testing and training needs a very robust cyber range environment. The NCR provides an environment that closely replicates real and diverse cyberspace with representative services, representative networks and protocols, and scalable network architectures in complex systems/chaotic environments in order to provide relevant training to CMF and Cyber Protection Teams (CPT).

IoT is growing our attack surface, our system's exposure to reachable and exploitable cyber vulnerabilities. Cyber/Smart Cities provide fertile ground for exploit and these vulnerabilities have to be identified and closed in development, and not after deployment of these systems. Further, cyber testing and training has to be conducted in a representative Cyber/Smart City environment.

**Army Reserve Cyber Operations Group (ARCOG) Cyber Protection Team (CPT) Training**

There are many challenges within both the Army Reserves and Active Duty in developing skilled cyber professionals. Within the Army Reserves, the ARCOG plays an instrumental role in developing and providing trained and ready Cyber forces under the CPT construct to conduct Defensive Cyberspace Operations (DCO) and Cyber support to the U.S. Army and other DoD and government agencies.

Within the Army there are few cyber trained soldiers. The Army, through its recruiting efforts, allows prospective recruits to apply to become a cyber soldier. The Army reviews these candidates' qualifications to determine if they are good enough to come into the Army Reserves or Active Duty with some of the attributes to pass through the training and become a qualified cyber soldier in a year or two. Additionally, within the CPT structure and methodology that emphasizes individual team training over individual training, there is a psychological evaluation conducted to see if candidate recruits would perform well in a team environment. If a prospective recruit is evaluated as to not being able to perform well in a team environment, then they are going to work out well on the CPT. Within the Army Reserves, soldiers come together on weekends and for two weeks in the summer. This is not enough time to train soldiers, and the Army Reserves seek to push its soldiers for a few more days beyond the forty days' requirement, which is taxing on both their families and civilian jobs.

Within the Army Reserve Concept for its Cyber Force, the Army Reserves is transitioning from its existing Mission Support Teams (MST) structure within the ARCOG into a CPT structure that consists of five battalions with two CPTs for a total of ten CPTs operating from ARCOG Cyber Protection Centers located throughout the country:

- Adelphi, MD (ARCOG Brigade/HQ and National Capital Region CPC)
- Fort Devens, MA (Northeast CPC)
- Coraopolis/Pittsburgh, PA (North Central CPC)
- Joint Regional Intelligence Center, Lackland AFB, San Antonio, TX (Southwest CPC)
- Camp Parks, CA (Western CPC)
- Bothell, CA (Western CPC Detachment)
- Phoenix Detachment, AZ (Western CPC Detachment)

The ARCOG Training Concept is a four stage, iterative process that includes an initial assessment of the individual soldier for fit, individual cyber training/development, CPT sub-team training, and CPT validation and certification. The majority of the ARCOG's cyber forces are enlisted (who are younger and more technical savvy), with leadership provided by Warrant Officers and Officers.

There are four primary types of CPTs, each of which has a different mission. These include the National CPTs (N-CPTs), Service CPTs (S-CPTs), Combatant Command CPTs (C-CPTs), and DISA (DoDIN) CPTs (D-CPTs). N-CPTs have a different pipeline than the other CPTs, who in turn have focus areas given to them by capabilities that they should be specialized in (e.g., ICS/SCADA).

The ARCOG mission is to train and deploy teams CPT, although each team does not have a definitive mission for what they are going to do. CPT missions will be defensive cyber operations, as there is NSA check off certification before any team can do offensive cyber operations, which is a lengthy, complex process that the ARCOG CPT is not well suited today to conduct. CPTs are increasingly being integrated with "all source intelligence," having both cyber and intelligence forces integrated and trained together. There are five teams that will comprise the CPT structure, the first two of which will be IOC by 2018, a monumental task. They include:

- Mission Protection
- Discovery and Counter-Infiltration
- Cyber Threat Emulation (Intelligence)
- Inspection Forces
- Cyber Support

The length of time required to train Army personnel under the Army's 17-Series Lifecycle Development creates substantive challenges for the Army Reserves, within initial training requirements approaching thirty-eight weeks. With current policies mandating that none of the "19 positions/billet slots" can be doubled upon IOC (2018), the ARCOG is now required to place an estimated 26 of its CPT troops through this lengthy training regime. Current recommendations include mobilizing personnel for a year to complete these requirements, a requirement that could create significant challenges and burdens for the Army Reserves.

# What are Cyber Cities – Opportunities and Challenges

*Mr. Robert Griffin, General Manager, IBM*
*Mr. Greg Falco, MIT*
*Mr. Matt Butkovic, Carnegie Mellon University*
*Mr. Edward Contreras, Silicon Valley Bank*
*CDR Pablo Breuer, Naval Postgraduate School*

During this panel, panel members and participants shared their perspectives on what a Cyber City is all about, the challenges and opportunities associated with living or operating in a Cyber City, the biggest fears in living and operating in a Cyber City, academia's research contributions to living or operating in a Cyber City, potential considerations for U.S. senior leadership to consider for living or operating in a Cyber City, and proposed current authority structures enabling cyber speed responses in the event of catastrophic failures in Cyber Cities.

**What is a Cyber City?**

A Cyber City is really based on perspective. There is a unique answer to this question for everybody. A Cyber City is based on who is in your ecosystem, who you interact with, and who you are dependent on. Whether it's a financial sector or an energy sector or technology or government, everyone has to understand their Cyber City. The failure or success of your Cyber City really depends on how well you can answer that question. It is unique to everyone who responds to this question, and dependent on how you know the concepts of what that city is.

A Cyber City is also a dynamic, built environment, with a dynamic built environment that actuates based off of input. It is living in 4D, where you can interact with your infrastructure. It is not just about data that you are pulling from things. It is the integration of IOT, and control systems, and robotics that make our world that we live in actually interact with us. That opens up a world of possibilities.

Cyber Cities are a promise of doing things more smartly through optimizing existing facets of the city at its core. It is doing transportation in ways that are more sustainable and efficient. It is using water resources and electric resources and energy resources more effectively. It is using large sensor networks to monitor and reduce crime. It is a number of related things, with terms that are nebulous but that we have a gut feeling of what this means. It is also about connectedness, about network aware devices and systems, and corresponding ways of managing those things to optimize the urban experience.

Cyber/Smart Cities are entirely interconnected eco-structure environments that are going to support the movement of re-urbanization. The challenge within this environment is on how we are going to deal with important things like precious resources and critical infrastructure protection, communications, transportation, and the free flow of water and resources. Smarter cities/cyber cities will increasingly use sensor based networks that allows for more efficient and more effective tasking so we can do things like precision agriculture to make sure people are well fed, provide more efficient transportation, and to make sure water is distributed to its urban populous. With the advent of IoT and IoE, the challenges become even greater with the aspect that everything outside of critical infrastructure and primary communications will be interconnected, which provides a whole set of new challenges.

Cyber Cities entail the use of automation to support the population density that we now have in an urban environment. Usually this conversation goes to power generation and power distribution, but there are other things like transportation, how we can get the amount of food needed to support to the population density like we have in New York City; how we get emergency services to the right place at the right time to help people; and how we embrace and effectively use automation, computer network sensors, and RF networks.

**Challenges in Living or Operating in a Cyber City**

One challenge is the ambiguity that the actuation of these environments allows for us, as we don't know how to predict the data we are going to get from these devices or what people are going to do with the data. We don't really know what is going to happen after they use data to interpret something. We lived in a pretty static world prior to 2000, where things worked one way and that is all they did. Now we get data from everyday devices, hack into their servers, mess around with it. We are living in a world of ambiguity and chaos, and now have to manage chaos. Within these cities, we have to think in ways attackers are going to think, and that is exciting.

Another challenge is complexity, and two levels. First, there is technical complexity. We live in a country who is struggling to keep physical infrastructure up and running. Many places are challenged to keep their bridges from falling down or to keep their lights on. The second is the complexity of integration, specifically on integrating this new way of living and working with an existing infrastructure. The life cycle of our critical infrastructure assets is very long. It is not that we can take things (e.g., sections of this architecture) out and just replace them.

Another challenge is actually two-fold, security and policy. The first, security, is exacerbated with the proliferation of new, undiscovered use cases or threat perspectives that are becoming more and more surprising to us as we start to evolve. The second is policy. For example, during the Boston Marathon bombing and shooting (terrorist attack), this was a tipping point for the use of video technology in this country and the reality behind that was that it was not government or city infrastructure that was obtaining most of the data, it was private infrastructure. A perfect view was provided from a facility (bar) across the street that captured when the bomb ignited. Security around the world is going to be an incredible challenge. Does the U.S. have the will and policy to take advantage of the private infrastructure?

Another challenge is risk, as we automate all these things without understanding the risk we are accepting. In a lot of cases when talking about cyber and smart cities, we are talking about infrastructure. Outside the cyber realm, engineers (electrical, mechanical, civil) are professionally educated and then get their license to show some proficiency. When we have a problem with the water system, the plumber that comes to your house is licensed. However, in the cyber realm, anyone can pick up a manual from Amazon and claim they are a software developer and then develop software for a transportation system or electrical power distribution or your pacemaker without any assurance of proficiency. We have a plan for failure and we don't engineer software for failure. Therefore, it likely our Cyber Cities will not be resilient.

A final challenge is that we are so dependent on areas that are outside our control or view. In order to move money from one place to another, we are depending on things that are outside our area of expertise. In order to do transportation from one area to another, same type of challenge. If you are thinking about Cyber, and everyone knows how hard the word is to define, think about all these things that have a plethora of information. You are dependent to get it to your final inputs and outputs, and understanding the interdependencies is one of the hardest challenges. Anybody can do it, and everybody is. Additionally, how do you get something out of it, as no one person or industry has the holistic solution?

### Opportunities in Living or Operating in a Cyber City

The first opportunity is the re-urbanization idea that we can take and maintain livable, massive cities on a scale that we have never seen before. It is about applying smart methods to improve the standard of living for those that are increasingly concentrating in these areas.

Another opportunity is power within interconnected city. With natural or manmade disasters, such as in Hawaii, it is critical to have power up and running effectively to keep water systems on to sustain life, keep lights on throughout these cities to places such as hospitals, and to move troops in and out. The ability to interconnect everything starts with keeping critical pieces of infrastructure up and running so we can seamlessly navigate across those elements.

Another opportunity is embracing the disruptors. If looking at Uber, they are considered both a technology company and transportation company. They are a disrupter that a lot of stable and static companies challenged. These static companies did not want to accept them into their industry. Uber did not care, and they entered the market any way. The opportunity is to look at and embrace these disruptors, as disruptors will continue to come that impact living and operating in Cyber Cities. One will likely not know that this disruptor is, or what industry is going to be disrupted, but any industry that has been static for a certain amount of years are targets of opportunity to disruptors.

Another opportunity is actually in the risk. When you have risk, you are forced to think what that risk is, and think ten steps ahead on what that risk can to do to you. When forced to think ten steps ahead, you have to innovate and do something real creative/innovative to fix or manage that risk. In a chess game, you move one pawn forward. If you have situational awareness and see what is happening around the chess board, you can surmise what might happen on the chess board with this one move. In a Cyber City world, you are moving all of your pawns ahead at the same time. This brings us collectively one step closer to our enemy. We are faced with thinking more quickly about all the risks that are happening, and it is happening at scale. The risk is the opportunity for us to think faster and further ahead.

A final opportunity is increased efficiency and sustainment. Our world’s population is trending towards 10 billion. Before farming, and interconnected cities, we could not sustain the food production required to support a large scale city like LA or Shang Hai or New Delhi, so really supporting the amount of human life we have now is the biggest advantage to these interconnected cities. This includes being able to get the right amount of food and water and electricity at the right place and right time, and having to move hundreds of thousands of people from where they live to where they work, and this does not happen without this level of automation. Most of us also carry smart handheld devices that allow us to access a sum total of human intelligence. This is a double edge sword, but provides tremendous opportunities.

### Biggest Fears in Living or Operating in a Cyber City

Scale was cited as one of the biggest fears. Within a Cyber City, scale is data, the interconnectedness of that data, and management of that data. Nobody can know what is on their computer at any given time. How can a massive organization such as the military be able to manage all this data at once? That is a tough concern, a fear, and a mess.

Another fear is the incredible contribution but one that we are not prepared for, the art of the possible. It is also concern about the generation that is building the massive applications to this world, the Millennials (Generation Z), who are the first generation born in the internet era that believe in an open society and do not have a substantive concern for security. They are the next workforce with an agenda driven by building something creative, and who contend that a lock down on security of this environment will stifle their creativity.

Another fear is that we continue to automate things without understanding of the basics of the fundamental limitations of how outdated most of us are, and we continue to accept risks without understanding the risks we are accepting. The choice is whether we stay with the status quo and just admiring the policy to make things better, or whether we start gaining ground to make things safer and more resilient.

Another fear is the speed of evolution. Nothing lasts forever, and actually nothing lasts for a short period of time anymore. The fear is not so much the things I do not know or things I do know, but instead this constant change by this evolution. If you want to become secure, you have to know your environment. How can you know your environment if your smart phone or other smart devices are always changing? If you don’t understand and keep pace with that type of technology, you should be afraid.

A final fear is unsecure massive infrastructures. The ability to govern this or to apply rational risk management is being outpaced by the technology itself. This does not mean, however, that because we cannot do this that we should not move fast ourselves. We are not good, as a matter of public policy, in anticipating what cyber cities will look like in three years, and for getting ahead of this before we see disruptive events.

### Academia’s Research Contributions to Living or Operating in a Cyber City

A first area for academic research is not looking to current predictions, but instead looking to 2030 predictions, where people could well have hybrid bodies (computers inside their bodies).

Another area is for academia to focus on foreseeable future. Industry is currently looking at (and working) 10 years into the future that academics should be working on. Five years is not too far out because evolution of technology is going to grow quickly. We need a lot of smart people to think about stuff that nobody has thought about yet, which is the academic’s role (with heads in the clouds). They need to be looking beyond the big problems we are looking at now, even beyond computer chips in our body, such as what is after that event and what nobody has thought about developing.

Another area for academia in creating next generation engineers that can solve these problems. We discussed skill sets required to do cyber. What more needs to be more done to anticipate the skills? Academia needs to play a lead role in turning out engineers who understand these system of systems problems that are essential parts to

Cyber Cities and Smart Cities, and at the practical level, ensure we are creating the skills and creating the pipeline of knowledge workers.

As data is not getter any smaller, academia should also focus on how do we more effectively move/push data to an exit or entry point (edge), and how to ensure we are getting access and distribution to content in a timely fashion that makes a meaningful as close to the point of the medium as possible.

Finally, academia should focus on both research and education. Few people today take a programming class, and even fewer get secure coding fundamentals. These should be an absolute requirement for everyone going through the educational system. It is not just about programming secure coding principles, that is on the education side. On the research side, for the mathematicians, there are fundamental things that we don't know or do not understand that we can't solve without a mathematical model. We also have no mathematical model or methodology for authentication. Yet all security is predicated on secure authentication, so we are building and building without a secure foundation. We have also been building computers based on Turing machine for over 70 years. There are fundamental limitations of the Turing machine that ensures we cannot solve any of the real questions we have about security (for example, we cannot tell if a program will halt at a given input). If a computer/smart device cannot tell you that, then they cannot tell you is something is malware, malicious, or a bad packet. Therefore, we need a new model for computation that is not based off the Turing machine, and we need a new architecture that works in an operational sense that is not based on Von Neumann architecture. Until we solve the mathematical model for authentication problem, the Turing machine problem, and the Von Neumann architecture problem, we are not going to get fundamentally better at security. This is a perfect area for academia to focus on.

**Potential Considerations (Regulation, Law, or Policy) for U.S. Senior Leadership to Consider for Living or Operating in a Cyber City**

A first consideration is to develop a policy for Cyber Cities the way the Internet evolves, which is more distributed and organic. A centralized policy for this Cyber City space really does not exist right now, and a centralized solution is not necessarily the answer. We need to have the individuals creating the future to help create the policy. However, we cannot create policy for governmental action of the future without first knowing where it is going, and we need to develop regulation that is not regulation. What that looks like in uncertain. If there is a way that we can start thinking about the way we are constructing this view of the future from a governmental perspective, the way that the technology is actually evolving and what is possible with that technology, that is what we would be looking towards.

Another consideration is having a more honest dialogue with the owners and operators of the infrastructure within the Cyber City, as the vast majority of these things are owned by private industry. There is currently a tension between private industries, who make assumptions about things that the government will live without, and the government, who makes assumptions about what private industries will do in defense of the nation. There are some strides recently in information sharing and other facets, but fundamentally, at the critical infrastructure level, there is no shared vision. We need to reset those expectations as a matter of national policy.

Another consideration is for the U.S. to ratify the Trans-Pacific Partnership (TPP), which advocates the free flow of trade and digital information. Of the twenty-two member countries, twelve of them represent 36% of the world’s GDP.  In this interconnected world, there should be no restrictions and constraints placed on the free flow of trade and digital information by any of the TPP members.

Another consideration is a recognition within the DoD that what the military services are doing with cyber warfare and internet warfare is not really working.  They don’t have dedicated professionals and clear career path. We ask our troops to support cyber activities and missions at U.S. Cyber Command (USCYBERCOM) or one of the service cyber components, then send them off to become another operational component where they function in different positions such as a Signals Officer. That means our forces cannot become technically and tactically proficient in Cyber.  Within the other operational domains, pilots want to fly planes, infantrymen want to be out in the field, and sailors want to be underway at sea.  Cyber forces want to stay on the keyboards, and we have to find a way to keep these cyber folks with tactical proficiency in the warfare area where they gain proficiency (i.e., cyber domain), or we are absolutely going to lose them to industry.  If the mission is taken away from them, they have no reason to stay.  In regards to Cyber, Defense and Federal Acquisition Regulations are broken, and does not keep up with cyber speed. We often get systems and capabilities that we do not want, never asked for, and by the time they get to us, they are obsolete and broken and broken and meet no mission need.  Those are things that got to change.

A final consideration involves regulations that give us a false sense of security.  Anybody who has managed a program and/or has worked with the regulators knows that you can get through any regulated exam by doing the bare minimum, and then officially be designated secure when in actuality you are not.  Anybody who has been an operator and on the keyboard knows for a fact that just because you have auto locks turned on does not mean you have protected systems or networks.  Regulation provides a false sense of security, as you cannot regulate a cyber domain that moves quicker than you can create laws. What needs to be done is to create an environment that allows companies/organizations to bring systems into a consistent or constant state of purification (whatever that looks like) only if they meet requirements.  If they do not meet these requirements, then they do not enter. Applying regulations gives a false sense of security, and gives executives a false sense of bravado and government a false sense of oversight.

### Does the U.S. Have Current Authority Structures to Enable Cyber Speed Responses in the Event of Catastrophic Failures in Cyber Cities?

Cyber speed is subject to interpretation. If history taught us anything, then historically we continue to struggle with kinetic events and catastrophic kinetic events. As for cyber events, do we as a nation truly understand where the authorities lay prior to and during a cyber incident?  Does the National Guard operate in a cyber emergency as they would in a hurricane or flood? What is the equivalent of filling cyber sandbags?  What is the role of industry?  There are a lot of authorities, titles, and command and control issues involved in responding to a potential cyber catastrophic failure.

Many forward-thinking companies are building their own intelligence units, and many within DoD and government (as well as in industry) recognize in the face of a cyber attack they are likely to be the first responders. They are not counting on having someone from the government or military establishment come in and solve their problems. These organizations are saying they cannot expect that when things happen that anyone will come in a timely enough fashion to protect its brand, its infrastructure, and its intellectual assets.

At the end of the day, industry needs to recognize who is accountable, responsible, and consulted. When these breaches occur, it takes so long to apprehend the individual(s) committing these offenses. Nobody is going to come to our (industry) rescue to help us out except ourselves. When you get these centers (small and large businesses) that are focused on their response (first responder), they are the ones to have the visibility, technology, and expertise to be those first responders. These organizations also can go out and say they can protect you, especially in the light that nobody else is going to do so. In looking at this question from a business perspective, someone needs to define accountability, who is responsible for consulting and informing during an incident, and who determines the level of catastrophe (internal to the company or one that transcends multiple industries), as each one calls for a different response.

Properly addressing catastrophic events is not a government problem or a company problem. It is also not every man for himself. It is more like every man for every man. Why should we limit these problems to trusted government entities or trusted companies, when we have the best hackers out there operating in their basements or from non-traditional organizations? Let us find ways to organize those people. The Syrian Cyber Army is a big threat to our nation and western world – how did they get their people? They have regulars in their basements learning code, and now they are helping out their government. The U.S. has people who are "boxer ready" and we need new models. It does not have to be the military or government to have an official response to a big cyber breach.

If there is a catastrophic event today, we would likely fail catastrophically. As to who officially is in charge, that is generally well laid out in U.S. law and title codes. The numerous U.S. titles and executive/presidential directives tell us exactly who is to respond in each way to which kind of event. What we are not doing is exercising these authorities efficiently. We have done a bunch of table tops, but we really have not done a large scale response to a catastrophic incident. The last time we had a large scale response to a catastrophic event was Katrina, and that was something that we knew was coming. We failed because we did not communicate well nor did we exercise for it. What we have is a good paper framework for how we should respond, but we need to exercise that so we can respond (and have confidence) as we should.

### Younger Generation Perspectives for Living and Operating in Cyber Cities

The younger generation generally does not trust the government getting access to industry data, even if it supports identifying and countering threats. The Millennials (Generation Z) is our next work force – they are generally less secure, much more willing to post information on the smart (albeit vulnerable) personal devices, and think that everything is okay since there is someone or something is out there that will take care of these problems. Most of this generation views having access to the Internet as fundamental to human rights. The millennials generally have no problem with giving Google all their data since they get many gifts such as Google Drive and Gmail. This could be related to Google being upfront with them in stating their intent to pass information on to various advertisement companies. However, millennials do get upset (as do many within the older generations) when they get lied to, such as when Lenova and Sony put back doors in their devices to monitor for piracy.

# Skills Required for Operating in a Cyber City

*CDR Pablo Breuer, Naval Postgraduate School*
*Mr. Jose Fernandez, Lead Scientist*
*CW3 Negron, 780th MI Brigade*
*Ms. Lori Pridmore, Lockheed Martin*

During this panel, panel members and participants discussed the challenges and opportunities associated with living or operating in a Cyber City, the biggest fears in living and operating in a Cyber City, academia's research contributions to living or operating in a Cyber City, some potential considerations for U.S. senior leadership to consider for living or operating in a Cyber City, and proposed current authority structures enabling cyber speed responses in the event of catastrophic failures in Cyber Cities.

## Skills Required for Operating in a Joint Force Cyber/Smart City

In discussing the skills required for operating in a Joint Force Cyber/Smart City, we need to first come up with a consolidated definition on what they are based on commonalities across these different definitions. Based on a synthesis from multiple sources, a Cyber/Smart City is defined as a city that can leverage integrated people, processes, and technologies to make near real-time information decisions in order to successfully achieve its objectives. In looking at executing full spectrum cyber operations in support of a Joint Force, we will need to modify the Cyber/Smart City definition.

A potential definition for our consideration is that a Joint Force Cyber/Smart City is a Joint Force that can leverage integrated people, processes, and technologies to make near-real time decisions in order to successfully achieve its mission objectives that includes:

- Counter terrorism and irregular warfare
- Deter and defeat aggression
- Project power despite anti-access/area denial challenges
- Counter weapons of mass destruction
- Operate efficiently in cyberspace and space

In looking at the individual skills necessary for our cyber warriors, they will need a combination of technical, analytical and soft skills. Technical skills include baseline skills that every cyber warrior should have, such as understanding operating systems, having basic computer programming skills, and understanding network traffic analysis. Technical skills also include specific skills, those additional in-depth skills that a cyber warrior needs to do their specific jobs. Network analysts have different skills than an operator, and operators have different skills than a forensics analyst. The next skill set needed are analytical skills, those skills that enable an analyst to step back and look at information and traffic from a discerning eye, and then make something out of the information. The analyst needs to be able to determine the so what, why would a Commander care, and why are you telling me about this? The last skill set are the soft skills, such as being able to actively listen and communicate with commanders and decision makers what you are seeing and why is it important to them, and why he or she has to make a decision based on what you are telling them. Other soft skills include work ethics, responsibility, positive attitude, professionalism and team oriented.

In order to measure the effectiveness of our forces, we need to measure our forces ability to operate as a team. Exercises gauge team readiness skills and ability to make educated decisions using the information, processes and technologies they have on hand. Exercises usually contain a few main events, involving tasks and sub-tasks linked to mission essential task lists, that a team must be able to execute. Some examples of exercises that measure the effectiveness of our force's cyber skills includes Cyber Storm (DHS), Cyber Guard and Cyber Flag (USCYBERCOM), and Cyber Shield (Army/National Guard).

### Skills Required for Operating in a Virtualized Cyber City

In defining (or characterizing) a Cyber City, one might look at this being something that is virtualized. Cyber Cities could be seen as models representing something that currently exists, but that is not limited to an actual city. It could be structures such as a large ship (aircraft carrier), international space stations or future space stations, or underwater stations. The city does not have to be physically located where we live or operate or walk to, it can be any form of structure that is complex enough. These cities are all interconnected, and have things that have some form of SCADA correlated for electricity, water, or gas, and something that remains its central focus such as buildings.

Within a Cyber City, if you need to change something rapidly, the framework/infrastructure needs to be flexible enough that if you need to make changes to it or add components, you can. If you look at a real city, there are many intricacies involved in such things as building a shopping center – you need to get a permit, get contractors involved, and build the center. This process is now something that you do not have to do, saving a lot of time and money, as you are not trying to replicate the exact city (creating real cities) but instead trying to build it to scale.

In the context of Cyber Cities and its application to military training, there are several vendors offering Cyber Cities to the military – these are different than cyber ranges. These Cyber Cities are more complex, there are more pieces to it, and they are trying to mimic some aspect of our society. In some cases, Cyber Ranges are more narrowly focused on trying to get some training objective or specialized task completed, whereas a Cyber City offers different avenues to approach and more things to do, which in turn increases the complexity of some of these training exercises.

Within the Virtualized Cyber City, you would have the ability to interact with something without having to own or have physical access to a power grid, sub-station, or devices (e.g., Siemens controllers). Instead, you can get an UPS and hook it up to the Internet and make it recreate/mimic the above by assigning them to different ports. This enables you to take complex problems and really scale them down for the purposes for what you are training. At the end of the day, if we are going to leverage Cyber Cities, we are trying to train troops to do something. It is really hard to get people together at the same place and the same time and with the same mindset. In leveraging Cyber Cities, you are condensing everything you want to train on in an exercise at one location, or that is accessible to all different sites in either a singular or continuous event.

The following are the three core skills required for troops to become proficient in Cyber Cities that need to correlate to the following three domains of Cyber – Computer Network Exploitation (CNE), Computer Network Operations (CNO), and Computer Network Defense (CND). These skills are:

- Dev Ops – to include designing, developing, deploying, and configuring hardware and software; process reengineering; and communicating and collaborating with others.
- Programming – which takes a lot of time to teach, and there is not usually enough time to develop proficiency.
- Systems Analysis – as related to a certain technology or platform, and it is pretty relative and broad.

It is very difficult to find people that are good at all the above skills. Additionally, it is extremely difficult to obtain and retain commercial certifications required to do the job, and usually an employer or military establishment won't provide sufficient time for users to keep their skills current. Troops usually have to make time for themselves or lose their skills and proficiency. If you do use a Cyber City, you need to have a narrow training objective with realistic scope and requirements.

**Skills Required for Operating in a Cyber City (DoD Test and Training Perspectives)**

With the increasing connectivity between all kinds of devices, there is a need for developing environments to conduct high fidelity tests and training. We need to become more aware of the implications of this increased connectivity of our systems, and on how we design and think about systems we develop.

When people first approached the NCR, they associated Cyber with IT. They did not think about weapon systems, or SCADA devices, or sensors. That has completely changed over the past four years. An estimated 80% of NCR testing is related to major weapon systems and platforms, and the integration of those things. The NCR has seen an evolution on how people view Cyber and how everything is connected, and how everything is related to Cyber, otherwise known as Cyber convergence.

Another implication on the environment in which we operate is the diversity of domains, which is increasingly becoming a very diverse mix of military, civilian, and commercial systems (e.g., commercial SCADA systems within a networked shipboard environment). Additionally, with increased connectivity, interoperability shifts to interdependence. This is about cyber convergence and understanding how we operate in a cyber interdependent environment. If you only think about your system and type of security you have on it, how do you operate your system and execute your mission in the absence of trusted data? This becomes is a system of systems problem, and that analysis is how the NCR changed its tests and thinking about the cyber problem to include both the major platforms and edge systems (end to end problem) and their vulnerabilities.

The NCR witnessed a shift from static design of cyber solutions into major systems. Initially, there were IA requirements and the NCR just checked the box. It was nice and easy in the past as contractors got those requirements, and the NCR validated the requirements. In a world where you cannot predict what the environment and threats are, how do you design and build a system for that? What the NCR is observing is that IA is not sufficient and is not scalable, and that there is a need for developing design techniques.

From a skills perspective, the NCR has a different philosophy on training. They do not have or train cyber engineers. When looking at testing and training, the NCR has software engineers, hardware engineers, and network engineers who all work together to give that integrated perspective, who collaborate together to produce a more resilient design, and who use a multi-disciplinary approach to designing systems. Many major acquisition programs would approach the NCR, and have their Red Team come in and report that this program/system had hundreds or thousands of vulnerabilities. That is not useful information, since the recipients of this information would not know how to prioritize and work on those that really need to be fixed, or know now to correlate these vulnerabilities to its mission impact.

The NCR is not just testing, but putting together useful products in design techniques, and making tests in design techniques, to gather data to inform the design as part of the engineering process. This includes more testing earlier in the process, and increased importance on getting mission critical information.

### Skills Required for Operating in a Cyber City (Academia Perspective)

We don't need to develop any new academic skills in order to effectively operate in a Cyber City. What we are not doing well is integrating these skills. In making smart cities smart, we are having computers talking to control systems talking to physical systems. We need to make sure that when we have a problem we have a concept or idea, we need to identity who else has a need to know, who need to know who else has the expertise that can address the problem or issue, and we need to know who else needs to know and who gets a vote. Part of that requires some lingua franca, as a computer scientist needs to be able to communicate with an electrical engineer or operations researcher or mathematician, and they in turn need to do the same. Some questions that they all need to know answers for are – What do I gain? What do I lose? What does it cost? As for cost, it is not just dollars. It could be operational friction. You need to know time cost, people cost, effort cost, and energy cost. If you answer those three questions you have to explain it in a language that someone outside your field and expertise can understand.

### Should Government Virtual Ranges Be Available for Industry for Their Exercises?

The NCR looked at how to apply their techniques to the private sector, and noted that industry's focus was different. Some companies have cyber intelligence centers and have developed their own cyber toolkits. These companies then embedded this into their culture. There is likely not a market for industry to use government virtual ranges. However, there is a market for companies in setting up a cyber monitoring/immersion centers center so they can monitor what goes on in their network and characterize threats and vulnerabilities.

Virtual cyber ranges have utility up to a point. It certainly makes it easier from a training perspective, but once you get to a certain level of proficiency, there are some inherent problems in virtualizing ranges. Nation state powers are aware of hypervisors (a piece of computer software, firmware or hardware that creates and runs virtual machines) and institute defense measures or act in ways different in a virtual environment. Gaining proficiency in virtual environments is of little use. The level of effort you get behind a training event goes along with the perceived level of emergency. The way one behaves when you know there are no real consequences is different than how one behaves if there are real, tangible consequences. So at some point you have to get out of the virtual environment and operate on real iron. However, there is some utility in the beginning stages the use of virtual environments for industry and government to train when there are no other ways to do so in geographically-disparate areas.

There is a lot of utility in using virtual ranges as a key element of industry's business practices and continuity plans. Industry should exercise in a virtual environment what they have in writing at the highest levels, and include this in their Business Continuity Plans.

There are benefits of virtualizing much of the equipment we already have. There are numerous limitations as to the amount of "things" you can out into a Cyber Range or Cyber City. Virtualization has a lot of advantages especially when related to Cyber Cities and training. There is a market that translates nicely from public to private sector. You do not need to train and exercise on a range set up with the NCR. That would be nice, but not a "must have." Industry could use virtual ranges for their team to exercise those processes in order gain increased insights as to when something happens, they would know how to react.

**Training Operators in Cyber Ranges**

It is important to give operators an opportunity to work in realistic environment, and see how individuals and teams interact. If an operator has a sensor issue, and does not know if it is a sensor issue or cyber attack, they can bring that up to the Network Operations Center. You have to have a training environment to be able to pull the full thread. We need to be open to the fact that there is not just one way to train an operator, as there are multiple different platforms that we operate today and that will pop up in the future. We have to train operators in a manner that lets them train on one platform and then if mission calls, allow for them to execute on a second platform. We have to have operators be able to transition between platforms quickly as the mission unfolds. We need to train our operators on multiple platforms based on the mission. The platforms being used within the U.S., and that we train on, oftentimes are not the platforms the adversary is using. So we need to train operators across multiple platforms to get the most out of them when mission calls.

Operators in other warfare areas operate symmetrically. Cyber does not. Cyber operates in a vacuum, and does not work. Cyber warfare is an asymmetric capability, e.g., you want to hack the killers, and want to kill the hackers. There are not a whole lot of hackers outside an aviation wing, and there is not a lot of anti-aircraft artillery in a hacker building located in Shanghai. The best one can hope for is a zero sum gain and you do not win wars and/or defend the homeland that way. We need to find a way to better integrate cyber operators with their kinetic operator counterparts. This will enable kinetic operators to call for cyber effects to meet their objectives, and cyber operators to call for kinetic effects to meet their objectives. We are not doing that.

Combatant/Component Commander exercises are starting to integrate Cyber Mission Force (CMF) teams as part of their operational tempo, and leverage CMF personnel and capabilities. Commanders are starting to do that, but if you look at Operations Plans (OPLANS), cyber operators are generally called in after the trigger is pulled. We can't sprinkle cyber at the end; we have to treat cyber operators like other warfare guys. We need to bring them into targeting boards. Now, the cyber operators need to be able to talk and walk like real warfighters, and we need a standard cyber nomenclature for cyber capabilities, both offensive and defensive. We need to be able to talk in Joint Pub 3 operational language.

Some large vendors have created Cyber Cities without marketing it that way, and focused on individual skills. Participants would be evaluated individually. This is a neat idea, but in the military you do everything as a team. Using this form of Cyber Cities creates challenges on managing groups of people working together on same exercises, and is not the most efficient way.

Mission comes first is a common phrase. If mission is the most important thing, then most of the "A-Players" will always be on mission. So when it comes to incorporating them into Cyber Ranges or Cyber Cities, many of these A-Players are taken out of the picture at the start. So in the whole team concept, if the team has to be divided in a way where cross training is essential, you need to be cross trained across multiple areas and multiple skills, but they need to have their specialization also. It is also necessary to complement the team with people with specialized skills in multiple areas in different fields, as team diversity is important.

## What do We Expect a Cyber Warrior to be Able to do to Support a Ground Component in Seizing and Holding Terrain?

What can a cyber component do to help out land warfare? It is not a question as to whether or not it is a cyber target or not. We need to know what is the objective and what effects do you need to have to support that objective? Given enough time, a cyber component can develop a resource to meet that effect. We should not expect a ground component to know what a cyber component can bring to the fight. A Commander should state their objective(s) and let cyber components figure out how to apply their cyber capabilities to give that an effect that meets their objectives. Most objectives can be supported given enough time. Cyber components need to know what the Commander's objective is, and then develop effects that satisfy those objectives and capabilities to meet those events. This is the right way, but usually not the way it is going to happen.

We need to be looking at cyber warfare commanders much like we do targeting, and we have to get the cyber guys in that same mindset of the operational forces and their targeteers. Cyber warriors don't want operators to tell them what weapon(s) to use, they want to be told what is the desired/required effect. However, how confident are operators/targeteers in the cyber weapon systems being able to get the job done. They may love Cyber Ranges and all its nuances, but how do they really know that a cyber weapon is going to get through the fog of war and achieve its effect. If is not exercised in a Combatant Command exercise, it does not matter. Cyber Flags and other similar exercises don't really matter to the Combatant Commander. Additionally, how confident are we in our cyber systems? If we cannot trust our sensors, how am I going to give you the information you need to act upon.

Within U.S. European Command (EUCOM), there are very few instances where cyber will be used for the sake of cyber. This will be a layered activity, and we have to normalize cyber like the other domains. We need to get to the point of having a combined set of kinetic and non-kinetic options, have to stop treating cyber as something special. Cyber has to be normalized from a tactics, techniques, and procedures perspective. Within EUCOM, there are exercises that CMF has proven its ability to be trusted.

However, within U.S. Pacific Command (PACOM), some targets within the AOR are hard to reach other than by Cyber. PACOM Commander have requirements do some things in Phase 0 and 1 that kinetic solutions are not going to help. For CMF teams to be used effectively and without hesitation, PACOM Commanders need to trust and have a complete understanding on how responsive cyber can be, and then get operational control (OPCON) of these CMF teams.

## Key Skill Sets Soldiers, Sailors, and Airmen Need to Operate and Live in a Cyber City

The first skill sets needed are baseline skill sets, like the Joint Cyber Analysis Course (JCAC), that helps students understand such things as programming, operating systems, and the science behind networks and wireless technologies first, then moves on to more specialized areas such as hacking, target research, signals analysis, network defense, and malware. Another key skill is obtaining an awareness of what they do and how that may impact everybody else. They do not need to know everybody, but they do need to who do to ask and how to get there. We need to teach our troops beyond their current task and how that gets you to the larger issue. Finally, our troops need to have humility and a willingness to ask questions, because if they see something and do not say something this could have a detrimental effect. They need to have an ability to ask questions and question the norm.

# DAY TWO – JUNE 22, 2016

## THE INTERNET OF EVERYTHING AND THE IMPACT ON NATIONAL SECURITY – THE EVOLVING THREATS AND CHALLENGES

## GOVERNMENT AND INDUSTRY RESPONSIBILITIES (CONUS/OCONUS)

*Mr. Jim Patterson, AIG*
*Mr. Robert Griffin, General Manager, IBM*
*Mr. Antonio Scurlock, U.S. Department of Homeland Security*
*SA Rafael Fernandez, FBI Infragard*

During this panel, panel members and participants discussed the roles and importance of Public-Private Partnerships, the cycle of adaptation of state and non-state actors, privacy and compliance, security versus generativity in U.S. economic growth, intellectual property, and cyber militias.

**The Roles and Importance of Public-Private Partnerships**

The U.S. Secretary of Defense, Ashton Carter, continues to emphasize the need for the Private Public Partnership Initiative (P3I), the ability for academic, public, and private organizations to come together to change (and continue to change) the game. We recognize as we moved from nation state threat vectors to market state threat vectors, the entire battlespace is blurring. Industry has an incredible role to play in that. Industry will advance and develop the advanced technology to support all communities, and much of the battlespace resides in private sector. How do we mandate how to bring industry's capabilities from a research perspective into this battlespace and partner closer with this community so that we ensure that our best interests are aligned? At the end of the day, the world has so changed since we became an interconnected society, and there continues to be a blurring on the lines on what is public and what is private.

It is important for the government, such as the DHS, to bring more of its partnerships together, to get more diverse audiences in the conversations they have, and to allow folks to give their operating forces an outlook that is different than what they have from inside the building (or beltway). Most folks don't know how difficult partnerships can be for the government, and how critical partnerships are shared between the federal executive entities. Many government organizations do have an operational, symbiotic relationship that works well, but there is a need to expand it further and ensure there is transparency in order for others to better understand how the federal government works in the cybersecurity realm.

Partnerships are critical, and what our company does is partner with its insureds to provide more than "here's your policy, give us a call after something happens." As for cybersecurity, our company has partnered with a number of outside vendors that hopefully our insureds can leverage at reduced or no cost that will hopefully reduce the risk of a breach from ever happening. With the number of claims filed each day, there is a lot of information on real time breaches. It is interesting to look at data and see how much it has changed even over the last few years. For example, ransomware was non-existent even a year ago. There are threat vectors that are completely new, and more partnerships are desired with the federal government and other entities to bring information together. However, many organizations are cautious of sharing this information for a variety of reasons. There is a need for clear parameters on what information should be shared and what risks an organization would face if they did share (need confidence in that they would not be putting them in jeopardy of additional liabilities).

In the past, Cyber Training for FBI agents was two weeks, and provided agents an opportunity to basically see what a cyber investigation would look like. Today that block is 1 ½ months. No matter what type of violation being investigated in the FBI, it is most likely going to touch some system and network. When training focused on cyber investigations, an instructor stated that one of the interesting things about how the FBI does business is that we say we have these cyber agents that are looking at computer intrusion cases. In winding the clock backwards, when a new violation came up we did not say we have phone names, we always had communications and this is not something new in how we conduct those investigations? One recommendation is for the FBI to consider turning a large number of FBI agents into cyber agents, for if these if you are working organized crime and doing white collar, you are definitely going to be touching your computer. As for public outreach, many people are very critical of agents. There are tons of sensitivity issues, and how does the FBI change that?

### Addressing the Cycle of Adaptation of State and Non-State Actors

From a Secretary of Defense perspective, the cycle of adaptation is quite rapid, and the threats we as a nation are facing are changing on a day-to-day basis. This validates the importance of partnerships, as there are a lot of different private entities that see certain aspects of it but not the bigger picture. It is important to bring all entities together to share the information they have to get the bigger picture, as this will help us to be prepared as things change to see the changes sooner rather than later.

The Secretary of Defense issued directives to the Intelligence Community (IC) to push them share more information. This is not necessarily about declassifying documents. It is more about the large swath of information that sits on classified networks that in and of itself is not classified that we should look to push down to the lowest level and get it out to the private sectors, and share the information with our partners. Do we share the risk of our adversary getting a little taste of that and doing something with that? We share risk anyway, and from a DoD perspective if we believe we are living in an environment that is constantly contested, then you are always going to have the plausibility that something that you are doing is going to be seen and observed or collected by adversary. We need to accept that level of risk into account, and then put the required (not necessarily all) information that are relevant to the public and private sectors out to the collective vice selective arena.

There are an amazing number of private firms that are doing some incredible things in support of the cyber/cybersecurity mission. There are forward leaning companies with an open source collection mission and young employees with Masters Degrees in Intelligence Analysis hanging out in Jihadist pages and chat rooms who are gathering and mining dark web information each day. These companies are then making this information available at a subscription based and patriotic level to a variety of organizations. The government needs to develop tighter and stronger bonds with these companies. Mission is evolving so rapidly, and few government organizations have the ability to focus 24x7x365 in all those sectors. The government (as does other sectors) has to be able to take advantage of those type of organizations from a partnership perspective, as well as a national security perspective. We need to try harder to define a space and role for the private sector in crisis management. They already have a role in Homeland Security but not a recognized space in national security. The private sector has had an incredibly strong and efficient role in helping during crisis historically. There are going to be different issues and interests at play in dealing with private and public entities, as private sector worries about brand while the government does not as an example. We need a quid pro quo situation. At the end of the day private industry has to do is report to shareholders. There can and should be a closer alignment between the government and industry, as it is impossible for the government given the role and challenges and resources in demand to service these problems. They cannot do it alone.

It is disconcerting to walk into government facilities and see how outdated things are. Innovation moves fast and it is going to be hard to keep pace with the technological advances, and we recognize that government it is not going to replace systems and technologies every eighteen months or so. However, it would be advisable to conduct a study of how old these organizations' equipment is from a technology standpoint. One such study was conducted by the DHS, who looked at physical and digital security systems. Much of the equipment was outdated, and not patched anymore once malware is detected. Folks then wonder how these intrusions happen? Well, they were still working on equipment from 10-15 years ago. The government will always need to invest in tanks, ships, and aircraft, but we have to recognize in going forward that we are going to have to invest more on our information and cyber systems with a realistic replacement program. What we do get is usually obsolete before it is even fielded. The Defense Innovation Unit Experimental (DIUx) is an outstanding solution to many of these challenges, but much more is needed.

**Senior Level (Notional) Perspectives and Viewpoints**

President Perspective: There is importance of getting buy in from the top. You can tell whether or not there is buy in from the top, or whether or not the entire organization is focused on cybersecurity, or whether or not each person in that organization is focused only on their little part of it but has no interaction to address the broader issue. The President, with his ability to guide conversation and make people understand what is important and what issues we need to be focused on, can drive things in the right direction that nobody else could.

Navy LCDR Perspective: As a Navy LCDR, I can lead from anywhere and talk to a Flag Officer, Chief Warrant Officer, and Chief Petty Officer. I can walk and go see anything I want and need to go see and see the problems that others might not want to see, and then be impactful in a short period of time. I have seen encumbered senior leaders who have multiple other concerns not be able to operate so freely. As a Navy LCDR, I have the ability to get the right balance of folks together at multiple levels and make marvelous things happen. I find the right partners, work late, and don't punch clocks to make it happen.

National Counterterrorism Center (NCTC) Director Perspective: I have an appreciation of the challenges faced by the NCTC, and from a mission perspective, consider that the NCTC has one of the most critical roles we have inside our country. The NCTC Director has opportunities to influence that role from a national perspective, and do things that are unheralded and not recognized from public perspective.

FBI Agent Perspective: Within the FBI, the rubber meets the road at the agent level. I wake up in the morning and don't know what is going to happen. Sometimes things go smoothly, sometimes not. There is a sense of camaraderie that after the dust settles, there are folks creating policy on privacy and security is left up to the country. We are here because the country wants us to do our job, which is sometimes difficult by design and needs to do as our actions oftentimes puts people into jail. It is about sharing intelligence, and when a crime is committed, we are going to be the people who respond to this. FBI Agents have incredible relationships with their Law Enforcement (LE) partners and generally get along with the local population. The FBI also has resources that can be brought to bear with smaller offices. What gets me excited and energized is always trying to do the job better and with higher quality people tactically doing their job, and how are we collectively getting better and getting trained.

**Privacy and Compliance**

There are always going to be privacy issues for the government, such as when the government needs to unlock encrypted devices. From the business side, if a company builds a device and puts a back door into it, they will likely become less competitive in the market place if this back door is identified. The government cannot force a Samsung or Nokia to go down that path and unlock their encrypted devices, and you can't regulate that. The government needs to work with organizations who has the forensics expertise and skill sets to do that. Let organizations such as Apple do their thing with protecting their brand and customers' perceptions, while coincidentally supporting those with technologies and expertise to break their phones.

We talk about when quantum computing is really here, but how quickly can we break encryption that is currently out there today? One of the biggest threats we have are encrypted devices, and things will go dark. There are ways the government can solve these challenges that differ than the direct way they took recently with Apple to gain access. Let's invest, support, and develop the solutions to do so, but let us not try to regulate.

There has always been a way for an FBI agent to get access. It is more difficult now, and search warrants are required, as the FBI cannot just break down the cyber doors. The FBI (and government as a whole) does need to develop access capabilities, and reach out to the partners. An interesting note is that Apple devices have been given to other governments, which in itself raises additional privacy and security concerns.

We cannot have 100% privacy and 100% security. Let's not vilify these companies for protecting their brand and the constituency they sell their products and services to.

**Perspectives on Security versus Generativity for U.S. Economic Strength and Growth**

Generativity is related to user having an independent (innate) ability to create, generate, or produce new content unique to a system without additional help or input from the system's original creator.

As a nation, our focus should first be on security, for without security, we are not going to have generativity either. If businesses are not able to conduct their business securely, then requiring a back door enables threats as well as the government to get into their devices and systems. This is a real concern. The better the security, the more solid the foundation will be, and better the business growth and generativity will be. When a breach occurs, significant costs are exponential (not an insignificant problem). When we see a substantive increase in the number of attacks on our critical infrastructure, security becomes the most important thing.

We need to focus on getting people to understand the risks. You have the ability to be more secure to the point where you secure yourself to the point that you cannot participate with others. If we do not understand what is truly of value to us, or we do not understand what assets or information we have, or we don't know what interconnections or eco-systems we share with other that are important to us, then we will have a hard time defining what it truly means to be secure. First, we need to know what we value. Second, we need to know who we value. Third, we need to know what information is valuable to us and them. To understand those things then being secured means it has to be layered, almost 3D (some aspects will be secure, some wide open). We are going to have to have two-way information exchanges that many not be secure in one direction while secure in another. Some things will be compromised, and we can only do best we can. Ultimately if I know this, and understand these priorities and prioritized risks, I can secure anything you want me too.

For the Millennial Generation (Generation Z), creating something new is so important, so generativity is of importance to this generation. We recognize the people that want to penetrate our systems have the ultimate pay for performance job, and given enough time and enough money, an adversary they can hack and break into most everything. The interesting thing about pay for performance is they don't get paid unless they are successful in doing it, and usually do quite well once they do get in. The reality is that if they do get caught, typically they will be convicted in an offense (non-violent crime), and will be back at it again soon. We might to focus more on encouraging and developing a creativity model, because creativity will solve all these problems. Creativity will help us become more secure, and will help us to become more effective in supporting and prosecuting the mission. If we stagnate any of that (generativity is to creativity as stagnation is to entropy), we will slow down, and others will be creative and more focused on that. We need a creativity model that will push security models.

Creativity will be the key to all the challenges we see. We see in the Silicon Valley all these folks creating. We need to have the same energy in the government workforce and people. We are creative, but we are not creative enough. There are always opportunities. There is no silver bullet for these problems, and we are always looking for what is the catch-all. What we need is an energy and folks that are creative. We need to identity and then develop them (people) versus focusing on canned solutions that are nothing more than shiny objects. The real solutions are not the shiny objects, but those individuals who are looking at something, who are seeing an anomaly, and seeing something flagged…and then trying to figure out what is possible. Generativity is key to creativity, and bringing that next generation folks into our fold is what is going to carry this forward.

### Developing a Well-Regulated Cyber Militia

Could a well-regulated Cyber Militia be developed that brings the collective creativity of industry and capabilities to bear in support of the government and armed forces cyber missions? One view is that finding volunteers would not be the difficult part. When are the events or activities severe enough, however, to bring those folks into the force and allow them to operate? How do we protect these militias, and ensure that these militias (patriotic force) do not cause unwanted collateral damage? Cyber Militias have always been in the government's and military's hip pocket, and there does need to be frank and open discussions that there may come a time when national and federal resources become exhausted, and that we have to allow the citizenry and their capabilities to help us engage an adversary that may be overwhelming.

### Protecting Intellectual Property

We need to ensure intellectual property is protected. Innovation is not necessarily stimulated by privacy in itself. It is stimulated by many dimensions such as profit motive and solving hard problems. In looking at the challenge of protecting an intellectual asset (commercial property), it is necessary to incorporate hygiene into our business processes. Industry will continue to develop things that gave them advantages in the market, and to keep those things close to vest until the company wants to make them available. Companies need to develop and apply strong hygiene rules, such as not discussing what is considered intellectual property on cell phones or via open email. It is important to conduct a set of secure conversations, and view yourself as a caretaker of this intellectual asset. What is hardest to prepare for and solve are the risks of insider threat, people wittingly and unwitting leaking this information.

# Cyber Threats to Domestic Systems

*Mr. Antonio Scurlock, U.S. Department of Homeland Security*
*Mr. Joe Grand, Independent Researcher, Grand Idea Studio*
*Mr. Billy Rios, WhiteScope LLC / Washington National Guard*
*Dr. Ernie Hampson, Van Dyke Technology Group*

During this panel, panel members and participants discussed countering cyber threats to U.S. industrial control systems, countering cyber threats through public-private partnerships and new models, embracing industry and academia support in cybersecurity, removing the barriers to identifying and publishing vulnerabilities, and professional challenges (operational and technical).

**Countering Cyber Threats to U.S. Industrial Control Systems (Navigating the Terrain)**

While serving in the Washington National Guard (WNG), most the members I serve with are people I work with in industry, and we do not get our skills from the military. The preponderance of my job is leadership and motivating the troops in the unit to do their job. It is hard to do military missions. Within my company, I do all sorts on real security assessment and penetration tests and all cool things, and can get to solving the solution in one day from time of call. When it is a military operation such as the WNG, it is more like six months. When government speakers state they are engaging industry, I do not know what you are talking about. I know some of the authorities to do cyber missions is still classified, but when I was in Iraq, I never had to go to the SECDEF to get approval to do anything. It amazes me. We should not be limited in effectively performing our mission is the ability or inability to navigate bureaucracy in the DoD or military. The DoD and government has a long way to go in collaborating with industry.

These hurdles are not only within private industry, it’s within the government itself. For those who can navigate, it is a shame to have to know a person in that organization to get things done quickly. We need processes that are not “persona based,” and it should be par for course that if there is a mission that needs to be done, we have certain authorities to execute. We need to execute these authorities alongside each other because the adversary does it that way. The adversary does not have bureaucracy. They have open communications and conversations about the latest techniques, they develop an attack list with the various tools they are going to use, and then they dare you to do anything about. Within the government, we are getting better at the conversation and in recognizing how bad it is, although not quite sure we work in an environment that is expeditious in meeting change. Even when you do, a lot of that expeditionary change happens under unique and good leadership and they always seem to rotate out when most needed. This is problematic for the government and DoD in that people with the right skill sets rotate out with little to no turnover provided for new person. The private sector has a leg up on that, as they provide continuity and pay folks to produce, unlike their government and military counterparts that have a process to rotate people every few years rather than keeping them in their profession and location where they can be most effective.

The government is like a completely separate world to industry. DARPA’s Cyber Fast Track was a pretty good innovation to get small companies and individuals to be able to work on projects that will help the government in some way. I did research that I do not know what the government was able to do with that, but I was curious about doing that research. There are some programs within DoD that are working, to include the Navy and Marine Corps who were looking to me (and others like me) to help further their skills in hardware hacking. So there are these groups of people within the government with lots of people with different skills, and lots of people who know things and some who do not, and there are classified discussions and unclassified discussions. Even within the FBI-Apple debacle, there were those in the FBI who had the capability to do what had to be done. So why was it then a big public thing within the FBI? Sure, we want to be more agile, but it is an impossible task to simplify it to a point that could enable for government to work with people outside of that (government) world. There was also lots of discussion about information sharing with big companies (the IBMs and GOOGLEs) in previous panels, but that is only part of that industry. The devices that are being installed and employed at installations for SCADA (and all these other cyber related electronic devices) are not only made by these larger companies. They are oftentimes made by small companies and by a handful of people with possibly military background, and includes those engineers who come out of school and develop something and then sell it into an installation. That is industry. It is not about the government getting in bed with larger corporations, but instead on how the government can get to the small companies to make them feel wanted, many of which do not know about security in the first place. Even if the government got involved to help them, there is this huge disconnect in designing a product and getting it working, and getting the required certifications, and getting the product tested. For these companies, designing it securely is a whole different thing. There are so many problems in trying to get everything aligned, and many would not even know where to start.

When some use hyperbole in talking about the grid and critical infrastructure being subject and open to attack by anyone with a computer, I do not think it is hyperbole. Our grid and critical infrastructure is indeed open to attack, and I contend that in many ways, cybersecurity is a myth. There is no real security posture or practice that cannot be countered by a dedicated hacker. However, an adversary needs three things for an attack to happen – intent, motivation, and opportunity or capability. The thing that might be saving us from widespread attacks against our critical infrastructure is that motivation may not be aligning up with the capability.

In looking at exploit development, there has never been a system that adversaries have looked at that they have not been able to exploit or penetrate. That is the same within the energy sector right now. When looking at the attack in the Ukraine, there was not a sophisticated attack put in place there, although there was sophisticated intelligence done before the attack. The attack itself was not sophisticated, and it was carried it out with a Microsoft Word macro. Many of the same old techniques are being used, and we are still falling for that. With this exploit they took down a significant part of their grid leaving 250,000 people without power. The only thing that saved them was the ability to go manual to get power back up. We know today that the U.S. does not have manual back-ups on most of its systems. So if our power grid goes down, it is not going to be for four hours. A tree falling in Canada caused a blackout across NE corridor in 2003. This was actually a cyber event – a tree fell, which caused an overload in the system, which then caused systems downstream to try to draw from upstream systems, and which then caused buffer overflows…all of which created a cascade effect that knocked out the entire power grid. So if a tree can do it, I am sure a human can figure it out as well. A monkey in Africa took out that nation’s power grid. In the U.S., we are not going to be able to defend the power grid. We can make it more difficult and we can make it more-costly for the attackers to do it. We have to concentrate on resiliency and manual back-up systems. In looking at the results of the Aurora Experiments, if an adversary were to take out turbines in U.S. power plants, there would be an incredible danger of not getting them up for months or even a year or so. We do not the back-up parts in place to replace them, and a lot of places we have to get those parts are the adversary that may have taken them out in the first place. If you look at projections as to how long it takes for people to resort to their baser sides, e.g., to wage war between populations for food and water, it does not take that long for it to get very ugly and for people to start to die. In meeting with critical infrastructure providers (e.g., oil, gas, electricity, smart cities, cyber cities), many are talking about connecting their business systems with their control side and ask about how to do this safely. They were advised not to do it. The fact that they talk about doing it is fiction, as they have already done it, as there are plenty of systems connected. Whether they were connected with another network down to the PLCs that were running the infrastructure on the ground is not known, but they were already connected. When you have a problem that can cause death and destruction at that magnitude, then you cannot connect business systems with their control systems on open networks. These companies are focused on running at lower operational costs and on competing better. Safety of the American people is not their first concern – they think it's the government problem, and not their problem.

A counterpoint to the above point is that the adversary might have the intent, but not the motivation or capability needed to conduct a cyber attack. For some adversaries (e.g., small countries), there may indeed be motivation and capability there, but possibly not the intent to conduct such an attack. There are many reasons for an adversary to have us think our infrastructures work flawlessly and are secured. The adversary might not want us to see how easily they move until they bite, observe us suffer with our degraded systems and networks, and back away hopefully undetected and/or undeterred. What also may not be there is the desire to take something away. For small countries, they conduct cost benefit analyses in determining whether or not to conduct a cyber attack. What they get out of that other than to do us harm might not be enough motivation to attack.

As for terrorist organizations, they certainly have motivation and intent but possibly not the capability (yet). What our nation does need to worry about is the rogue actor whose only desire is to inflict damage and terror, and then getting the capability to also attack. These rogue actors do have to find (and fund) the right attackers to support their aims, which may be easier when focusing on criminal motives, but likely more difficult when motives are to kill thousands or millions of people within a targeted country.

For nation states and actors with great motivation and capability, there is no real way for us to know where they are in our systems and what access they have. They will likely sit tight until they really need to move. Even if nation state could take down a portion of the power grid, would they want to because that means all the computers are down? If they have their fingers into our networks, why bring it down? Terrorists on the other hand would definitely have the motivation to take down a portion of our power grid or other critical infrastructures. As for the adversary getting capabilities to do harm to our critical infrastructure, they do not have to be that capable, and that is the problem. Whether it is our power grid, weapon systems, or military systems, it does not take much for a determined adversary to find a way into the system, reverse engineer a piece of hardware, figure out how system works, inject malware, and have it fail. As for terrorists, so much public information is out there already that it may be that their motivation to develop a capability that may not be on the streets yet, but not that hard to develop and employ.

There are many who contend that the Internet is resilient, while others do not. There are already individuals and organizations possessing the requisite skills and tools that have claimed they could take down the Internet within hours, which at times creates huge media frenzy. Disbelievers cite this is not the case, as use as their reasoning that the Internet has not been taken down. It is more likely that there are few motivations for someone or some organization to "defecate in their own back yard." However, just because something has not happened does not mean it is not possible for these individuals or organizations to do so – they are just waiting.

For those individuals and organizations having the intent and motivation to conduct cyber attacks on our power grid or other critical infrastructures, it is relatively easy to find a low cost, remote exploit capability (or someone) to wreak havoc. As for conducting large or targeted cyber attacks on or through the Internet, with its billions of advanced/specialized cyber systems and devices connected to it, you have to have a substantive depth and breadth of knowledge on how all these systems work, and what is required to exploit them. Finding a remote exploit for smart phones and devices, e.g., iPhone, is not easy, although not impossible (e.g., Cellebrite). Finding a remote exploit for previous versions of Windows, such as Windows 7, is also hard. Those are the nuances that our nation needs to talk about and needs to understand. For instance, if someone brings to your attention that someone used a remote iPhone exploit against one of your people, you need to know that person spent a lot of time and money on this and is willing to burn something that is really valuable, as opposed to someone employing an exploit to get access to a SCADA system.

Field Grade Officers and Senior Executives in the cyber mission area should never start a sentence with, "I'm not technical, but…" What that is telling me is that you really do not understand how to assess risk when it comes to cyber operations and activities. There is a lot of risk out there within the cyber realm, and being able to understand what level of risk you are being exposed to is really important. When someone brings to your attention that there are multiple ways of an adversary to penetrate your system, or enumerates how they can run exploits against parts of your weapon or IT systems, it is up to you to understand what this means to your mission, your weapon system, and your troops. If a Field Grade Officer does not have the foundation to understand what that means to them, then they are lost. They will then be more apt to spend scarce dollars unnecessarily on the latest cyber system and technology that will not have a measured effect on the security and/or resiliency on their weapon or IT system, which makes no sense at all to someone who knows what is actually going on. If leading cyber troops, Field Grade Officers have a responsibility to get and retain the right foundation to be able to fully understand the myriad of risks.

A counterpoint to the above is that it is okay for Field Grade Officers and Senior Executives to state that they are not technical, as that does not necessarily mean they do not understand everything their troops are doing, just certain things that they are not doing. They may have not done programming or operated any offensive/defensive cyber tools, but they could understand people, processes, things and how to assess risk based on what is presented to them, which is all you can do under certain situations. While they might not be technical, they still may have the ability to understand the capability being brought to bear and understand your decision processes.

## Countering Cyber Threats Through P3I and New Models

The DoD recently invited the commercial sector (vetted hackers) to test DoD's cybersecurity posture under its "Hack the Pentagon" initiative, the first cyber bug bounty program in the history of the federal government. Once hackers were vetted by an independent third party, they conducted vulnerability identification and analysis on the DoD's public webpages over a twenty (20) period commencing in April 2016. Critical, mission-facing DoD systems were not part of this program. The results were positive, and many of the findings have been acted upon. Could this model work, however, on our domestic systems?

There are companies, such as Google, that have initiated similar programs using similar models against web based applications accessible to internet. However, this model may not be the one to test IoT devices such as industrial control systems, or the power grid, or weapon systems within an IoT/IoE environment. We would need a different model.

There would likely be problems in using this model in the private sector. There are many individuals (e.g., ethical hackers) and organizations in the recent past who identified vulnerabilities and then brought this information to the appropriate authorities within those organizations in which they were found. Many were threatened with lawsuits to shut up, or many just covered their ears, or many pretended that harm is not going to happen. The fact that the DoD Bug Bounty program was successful is great, and it was great to see DoD put value on the research by independent researchers. If DoD did a bug bounty program on its mission critical systems/weapon systems to help make them more secure, many would jump on that, as it would be a physical instead of a remote access thing (this would require a sandbox environment). However, just because DoD (or any other organization) offer a bug bounty program does not mean this translates to a stamp of approval to say that "if nobody finds a vulnerability, then we must be fine." These programs are definitely making things better, and help in getting low hanging fruit lopped off the tree. However, we do need to acknowledge the fact that if someone does sponsor/support a bug bounty program, there are still going to be exploitable bugs that either someone does not find, or that someone finds and decides not to reveal.

For U.S. citizens (e.g., researchers and ethical hackers) to be involved in similar DoD and government efforts to conduct vulnerability identification and analysis against mission critical systems, weapons, and infrastructure, proper vetting and clearances are going to become increasingly important. There are many folks within the U.S. with the skills and talent to help out the DoD and government in this area. However, the vast preponderance of these folks do not want to even go through a simple level one process for ensuring you are U.S. citizen without a criminal record.

### Embracing Industry and Academia Support in Cybersecurity

The DoD and Government may actually be doing a disservice by putting so much money into cybersecurity. What they are doing is creating an industry that is out to make a buck and is selling/hyping their "secure solutions" with a lot of repeated systems or processes with new names, or that provide incremental changes to security that is really not giving you more security, but most of which are giving organizations who operate electrical stations or oil pipelines a false sense of security and confidence in connecting their business systems to their operational networks.

The DoD and Government should consider using more Cybersecurity Broad Agency Announcements (BAA), as they request targeted cybersecurity solutions. They also should consider more open research requests and make them easier for industry and academia to respond to, to include using challenge formats where they set a problem and conduct a contest to identify those non-orthodox organizations (and individuals) who can solve that problem. There are a lot of highly talented and industrious people out there that may not have that entrepreneurial spirit to go out and start a business; however, if DoD and Government put a contest out there and offered a large prize, e.g., $10-$20 million, they could likely obtain more optimal solutions at a fraction of what they would have paid for in hiring a defense contractor to build their system. These individuals and smaller (non-orthodox) organizations see that as a different type of challenge – if they solve the problem, then there is a big pay day at the end. The DoD and Government would be inspiring people and enabling them to create innovative solutions at a far lower cost than what we have seen in the past. As for DoD programs such as Bug Bounty, I think that vulnerability testing has limited value. The benefits are that you do have to get low hanging fruit out of the way, but that does not make you secure. For one thing, patching holes can create new holes, it's a moving target constantly. Sure, organizations feel better when bugs are being found and when the rate slows on the easier exploits against your system. However, this does not make you secure and in some ways you may be making yourself less secure, as the community has seen patches that have opened up huge holes in systems.

The Bug Bounty program (model) has definite utility to the DoD and Government. When the WNB performs its missions, they never start with a list of tools. Instead, they start by having the right people on the mission first. If the WNG get that rights, it does not matter what tools they have as they are going to figure it out. With models such as Bug Bounty, they are not telling you what tools to use or how to go about doing your job. They are just saying the DoD is opening this up to as many people we can, because maybe we will get the right people. When we are thinking about cybersecurity solutions, there are definitely things that our security solutions make a difference. The more important part of the solutions, however, is having the right people. Let them do the right job, and place less emphasis on tools and solutions.

**Removing the Barriers to Identifying and Publicizing Vulnerabilities**

There is a lot of research findings highlighting the vulnerability of our autonomous systems, such as FDA approved medical devices, to security breaches potentially impacting the safety and effectiveness of the device for what many consider a public service. There is also an increasing number of advisories and security discussions focused on lawsuits and jail time for bringing this to the attention of the authorities and population.

There are a lot of independent security researchers engaged in identifying vulnerabilities getting surprised when they read articles of authorities (e.g., FBI) raiding the homes and seizing property (e.g., computers) of these individuals when they do find a vulnerability. What happens when the FBI raids a security researcher? Well, independent security researchers stop helping companies identify and fix flaws in their systems. This recently happened with an early-morning FBI raid on a Texas dental computer technician who identified and reported vulnerabilities in dental patient management software to CERT. If we eliminate the surprise piece of conducting security research, and not "punish the messenger in the process of this research," we will go a long way to incentivizing more research. For every action there is an equal and opposite reaction.

There are also folks finding software vulnerabilities and are afraid of disclosing them at Black Hat conventions for fear of getting fired or arrested or raided. In response, many of these folks started going underground and found out that they could make a lot of money from selling that vulnerability to middlemen (good or bad) who made even more money. This raises a situation where our nation (authorities) are almost creating that hostile environment, and scaring the researchers into going underground. There is obviously an ethical boundary crossed by these individuals when they go underground, but this is their job and they need to decide on how dedicated they are on sharing this information for "common good" and face potential repercussions, or on making a living in the underground. We need the public and private sector to acknowledge that it shouldn't be a surprise if someone finds a vulnerability in an infusion pump. The response should not immediately be the FBI raiding these researcher's homes, but possibly instead telling these researchers to give a presentation and teach us their mindset as to how they did this so we can acknowledge this and find the bad guys doing this anyway. These security researchers are publicly presenting these vulnerabilities, and finding vulnerabilities that will either eventually be found by someone else or have already been found and possibly been exploited by someone else. The authorities need to recognize that security researchers are not creating the problems, they are just bringing them to light. The focus instead should be on the vendors not taking responsibility and accountability for these vulnerabilities. In making this worse, there is no real disincentive for these vendors to engineer security into their products or acknowledge/fix these vulnerabilities once identified. Many companies have been subject to cyber attacks or hacks, only to then see their stock price goes up. With no real financial motivation for companies to take responsibility for their problems either, in a way it comes down to security researchers conducting "research for free" under a fear of prosecution, or going down the dark path as nobody wants to get raided. Security researchers want to share information, and most of them are passionate about computer security and want to educate people who don't have the insight into this world. There is a huge disconnect. Our government and public-private sectors need to welcome the researchers somehow (the good ones) and shun the bad ones, and don't throw away good talent and good people during the process.

Academia should lean forward to draw "researchers that are not part of an academic institution" into their fold, to include assisting them to work within government processes and helping them do legitimate research through mechanisms such as grants. Academia in large do not attend Black Hat conventions of Def Con competitions and reach out to participants with offers to align attendees' veins of research to legitimate government research that prevents them from getting cuffed for not following proper procedures.

Within the "non-government" cyber community, what is considered legitimate is much different than the government's definition of legitimate. What is happening in the cyber world is that most security researchers/ ethical hackers are not academic, and they are not going to follow the traditional academic or government research process. Among these folks there is an anti-establishment mentality that still wants to do good, does not want to work with an academic institution, and instead go to a Black Hat convention and disclose the fact that they hacked a car or medical device without documentation or formal process or paper filing. The challenge for the government is identifying how to get these individuals and groups who operate in basements and underground, and then incentivizing them to share their information and techniques that affects the government without going through these other channels (or putting them in jail).

There needs to be some middle ground, such as the government offering these folks some protection, some middle ground, when they are sharing their research results to the government without having to go to jail (e.g., providing a get out of jail card free). Academia could serve as a third party bridge between white glove, institutional research and this other honest, holistic research but conducted at the edge that makes institutions like the FBI concerned. An alternative approach is for the government to incentivize and offer immunity up front to those individuals (who are often hassled for even doing legitimate research) with going directly to the government, or going to government before disclosure (full or partial).

## Professional Challenges

One professional challenge is trying to be an entrepreneur from inside a large company. In an effort to innovate and create new ideas, an entrepreneur often comes at odds with leadership and direction in the way they want to take the innovation. They are focused predominantly on developing new customer bases. Corporation gravity will always pull entrepreneurs back inside, and put you under the large corporation bureaucracy. This will slow down innovation and lead them to hit the brake on innovation when they should instead hit the gas. As cited in the Innovators' Dilemmas book, market leaders often succumb to disruptive technologies because they are not willing to break from what their customers are telling them what they want.  Large companies will not move without getting that customer feedback stating they want that new system or technology.  Innovation comes from providing customers with things they do not know that they want yet, and often you have to start in smaller scale and smaller markets. You have to build it up, and your larger customers will want it once after other people have shown they want it and that it works, and that other companies are adopting it.

A professional challenge for military officers in the cyber community involves transitioning between being a cyber professional and serving as a traditional military officer.  If military officers cannot separate themselves from the technical dimensions of their missions, they won't get to the important leadership work they need to do. Our troops need the opportunity to do their job, and as officers, if we can enable them to do their job, we are more valuable to them than sitting at a keyboard.

Another challenge is trying to spur change and change mindsets of people about the good side of hackers versus the criminal or adversarial hacker that you normally hear more about in the media. There is a benefit in what ethical hackers do, and that is a challenge for us on a day to day basis because our whole business is about doing that.  Independent researchers need to hear that the information and training they provide to the government and DoD has a positive impact on their organization and accomplishment of mission – many do not get the message.

A final challenge for those working in government is not to lose sight as to who we work for – the citizenry of this country.  We never can lose sight of that.  We need to focus more on how do we make it better for those that come after us.  Many in our current generation have no concept of the adversary and current threats to such things the IoT, IoE, or cyber sovereignty.  We need to enjoy these things as much as we should want to protect them. We need to walk that fine line, and regulate that with the ultimate focus on how a certain policy is good for our nation and citizenry of the U.S.

# Smart Grid and the Internet of Everything (Stitching a Big Data Patchwork)

*Mr. Robert Spousta, PACOM Sensemaking Fellowship*

During this presentation, our special guest speaker shared his experiences and perspectives as a civil servant at U.S. Africa Command (AFRICOM) and OSD; renewable energy generation, IoE, and Big Data (technology trends and resilience impactors); and PACOM Sensemaking Fellowship Program activities in Hawaii.

**Experiences and Perspectives as a Civil Servant**

Within AFRICOM, one of their challenges since standing up in 2008-2010 involved performing complex missions and delivering functionality that did not exist in a conventional infrastructure. This included how AFRICOM did such things as Public Private Partnerships, Interagency Coordination, Strategic Communication, and academic engagement. It also included such tasks such as writing an Interagency Communications and Coordination Annex to a Campaign Plan. These activities emphasized the importance of being very clear in terminology and the danger of ambiguity when we discuss such things as Strategic Communications, but also such terms as Big Data Analytics and Internet of Everything (i.e., the need for a lingua franca).

Within the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD SO/LIC), the Partnership Strategy and Stability Operations Office had a primary mission focus on Civil Affairs. Senior leadership successfully managed its Civil Affairs top-down/bottom-up dynamic that included heuristic and algorithm insights, and the Political, Military, Economic, Social, Information and Infrastructure (PMESII) model/analytical framework.

- Guidance from the top down is like heuristic insight, which is general by nature, and doesn't always translate neatly in specific tactical environments.
- On the other hand, feedback from tacticians to higher headquarters is like algorithmic insight, which is specific by nature and builds upward from many particular observations.

In any organization, there is a danger that real messages will be lost in translation and transmission, specifically that the needs of operators and tacticians on the ground are not making it back into the strategic needs of an organization. There is a need for both heuristic and algorithmic reasoning. When we talk about algorithmic reasoning, we are gathering a bunch of specific measurements in a very certain and prescribed area, looking at different variables, and collecting information over time to build up to a generalized rule of thumb. Heuristic reasoning takes the general rule of thumb for knowledge or wisdom gained over a period of time that is very general in nature, and then applying it down to a very specific situation. They are both important to data acquisition, data analytics, and insight visualization, and are key tenets of Sensemaking.

Within the Partnership Strategy and Stability Operations Office, both leadership and personnel used PMESSI framework for planning and research. PMESII disaggregated complex problem sets into a way that someone can go through the planning piece by piece and make sure they addressed problem sets from a multi-perspective aspect. Of all the PMESII variables, information and infrastructure were usually the most undermined, which led to questions as to what aspects of infrastructure are most critical as well as information, which leads us down the road to the electrical grid and Internet.

**Renewable Energy Generation, Internet of Everything, and Big Data: Technological Trends and Resilience Impactors**

When talking about vulnerabilities, we are drawn back to what happens when the lights go out. Within the PACOM Sensemaking Fellowship Program, the "I" of the PMESII framework involving "Infrastructure" led us to view electric grids as our single most critical infrastructure. Upon analyzing the many challenges associated with managing electric grids, we identified the integration of renewable sources as a critical trend, which in turn led us to the importance of detecting the formation of unintentional electrical islands as a key capability.

For critical infrastructure systems and infrastructure to be resilient, they need to be able to respond adaptively to changing circumstances. The Maginot Line in WWII represents the danger of inflexibility, while natural adaptations in nature give us lessons on how to be more resilient.

Smart Cities and Mega Cities are being built around the world that rely on data from a host of sensors and energy. Big Data has six facets - value, variety, volume, velocity, veracity, and volatility, but the 6V's aren't an established standard. The U.S. government and other consumers of Big Data must do a better job of establishing standards for data management.

Since the 2015 Climate Summit in Paris, world leaders have recognized that climate change is a danger to mankind, and that we have to generate cleaner power through solar, wind, and other renewable energy. The problem with renewable energy, however, is that it introduces instability into grid systems, because it is intermittent, and the distributed generating sites can become islanded, whereby they become disconnected from the grid network, but continue generating power.

**Hawaii – A Living Laboratory**

The PACOM Sensemaking Fellowship Program selected Hawaii as the initial testbed for the Synchrophasor Analytics System for Archipelagos (SASfA) Project because it is a particularly strategic location in light of the U.S. pivot to Asia. With Hawaii being a set of islands, it represents a bounded problem set and its power system displays unique characteristics as compared to the North American bulk grid, namely low inertia and low black start-quick start ratio, high energy costs, and aggressive renewable integration agenda.

The SASfA Project combines two technologies: Phasor Measurement Units (PMU) and Machine Learning. PMUs are used for a variety of tasks in power system operations, including islanding detection. Detecting islands is a critical capability for maintaining system stability, which is both data-intensive and complex. Detection methods must be sensitive enough to detect islands under a variety of conditions, and stable against false detection during conditions that resemble islanding. The most significant measure of a detection method's accuracy is the size of its non-detection zone (or NDZ) in which indicating variables do not fluctuate significantly enough to indicate an islanding scenario. Machine Learning helps us detect electrical islanding events by prioritizing computational resources, just like an Aegis Combat System detects incoming threats and prioritizes missile launches accordingly.

What makes the Sensemaking PACOM Fellowship Program unique is that this is a public private partnership with students (in a conventional sense) that have almost a client – client partnership with other organizations like the Hawaiian National Guard. The Hawaiian National Guard has come to us with problem sets which translates immediately into a research and dissertation. IBM helps us to develop the machine capability and analytic component. Another industry partner, MetaTech, developed phasor measurement units for the synchrophasors. Phasors by itself is a complex number that is derived basically by taking variables in a power circuit like voltage and frequency, and translating those into a sinusoidal waveform. While SCADA conducts a measurement every few seconds, synchrophasors can record up to 120 measurements per second, thus providing a tremendous advantage in our observation space and providing a magnifying glass into the electrical power grid. PMUs are being deployed increasingly within corporate America and across the world, largely in result to the 2003 Blackout in the U.S. North East. At that time, power companies spent a lot of time trying to identity to conduct analysis of what and how it happened. Part of the reason it took so long for the task force to come to its finding was that measurement tools at that time did not have a time stamp which made it difficult to cross correlate what was happening at what location and at what time. So when talking about fractions of a second, having a time stamp is critical to responding but also in analyzing data and preparing lessons learned and moving forward.

There have been millions of articles published focused on over a hundred distinct ways to do this phasor computation, such as looking at frequency, voltage, rates of changes in frequency, phase differences, and multiple other factors. All of that is feeding our analytic engine which has a computing capability centered on a computer doing its computations faster and learning how to do computations over time that has to start somewhere. For us, it starts with the brain system, its corpus of knowledge, and so we are still at a point where we have to identity what each of those algorithms can do in a qualitative assessment of which ones are different.

This leads to our research into the IoE and Smart Cities and Smart Grids – people, data, things, and processes. In looking at the consequences and implications, the important thing is data. Within the information age (and revolution), data is the raw material using technology to derive information, as is data about data, and the veracity and velocity of data. Data should be treated as the precious resource that it is.

We need to understand what cyberspace is and what is means for military applications, and that it certainly is a battlespace. At the same time, cyberspace is also a slightly special category, a virtual environment that the Laws of Gravity do not apply. Our computational capacity is increasing but our capacity to digest all this information has not been increased at the same rate, so that has resulting in increasing the large gap between what we are making (more data) than we know what to do with it.

When talking about cybersecurity, these are complex software problems, not easily solved. While physics deals with terribly complex projects even at the fundamental particle, software engineers must deal with arbitrary complexity forced by the many institutions and systems which switches and interfaces must confirm. These differ from interface to interface and from time to time, not by their specificity, but instead because they are designed by different people. In some ways, the IoE (with a focus on the Internet) is a misnomer, because a lot of machine-to-machine communications that exist through non-IP protocols and our current low system Input-Output (I/O) growth is a critical gap that prevents us from using data fully (i.e., generating more data than we can process). Smart Cities is not a new concept, and if we want to move forward and make them smarter, we need to focus more on the data.

# CYBER SOVEREIGNTY ETHICAL AND LEGAL CONSIDERATIONS

*Ms. Liis Vihul, NATO Cyber Center*
*Mr. Jeff Kossef, U.S. Naval Academy*
*Dr. Bradley "BJ" Strawser, Naval Postgraduate School*
*CDR Elliot Oxman, Department of Energy*
*Mr. Nate Cardozo, Electronic Frontier Foundation*
*COL Adam Siegler, 335th SC(T)*

During this panel, panel members and participants discussed sovereignty in cyberspace from an International Law perspective; freedom of expression, rights to privacy, and sovereignty in cyberspace; DOE cybersecurity coordination (U.S. and Canada grid cooperation); ethical cyber warfare and Just War theory; restoring trust between the U.S. government and private sector; deterrence in cyberspace; rules of engagement for cyber warfare; and establishing international norms on the protection of intellectual property.

**Sovereignty in Cyberspace**

There is International Law but no definition for Sovereignty for Cyberspace. However, there is a well-accepted "Principle of Sovereignty" that dates back to 1928 between the U.S. and Netherlands (Island of Palms Arbitral Award).

> *Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.*

This is a definition that is still being looked to by international lawyers today. There are other people who look at sovereignty from a cyber context – and think this new phenomenon altered the traditional understanding of sovereignty. There are those that think cyberspace it outside the reach of the sovereignty of the state. In an excerpt from "A Declaration of the Independence of Cyberspace," John Barlow stated the following:

> *Governments of the industrial world, I ask you of the past to leave us alone. You have no sovereignty where we gather. Cyberspace does not lie within your borders. Do not think you can build it, as though it were a public construction project. You cannot. It is an act of nature as it grows itself through our collective actions. We must declare our virtual selves immune to your sovereignty.*

John Barlow seems to claim that cyberspace is outside out of the reach of the sovereignty of the state, in other words, he claims cyberspace is something akin to outer space, the high seas, or international air space…areas in which no state can ascertain sovereignty.

In a speech at the Second World Internet Conference, statements from the President of China, Xi Jinping gained a lot of traction in the international cyber community when he refers to cyber sovereignty. President Xi Jinping called on countries to respect one another's "cyber sovereignty" and different internet governance models. He specifically said that the international community should respect the right of individual countries to choose their own path to cyber development, model of cyber regulation and participate on the same footing.

Strictly, from an international law perspective, sovereignty still remains a territorial concept with territoriality is still at the heart of this principle. This means the state's territory – its land area, its airspace, its territorial seas, its seabed and underneath subsoil, internal waters, and its archipelagic waters of its archipelagic states – are all subject to a state's sovereignty.

The Tallinn Manual process sought to interpret this concept of "Sovereignty in Cyberspace."

In using an analogy, when you have Russian tanks crossing the border into Georgia, that was a clear violation of sovereignty. It also was a use of force and an armed attack that entitled the target state, in this case, Georgia, to respond with force. From a cyber context, most cyber operations do not rise to that level.

So what about all those cyber operations against a target state – are they lawful or unlawful under international law? When does a state's cyber operations constitute a violation of a state's sovereignty? First, only a state can violate the sovereignty of another state. When you have a terrorist attack, that is never a violation of a state's sovereignty nor a violation of international law (although there are remedies available under national law).

Precise thresholds are unclear, and need to caveat this discussion in the fact that legal analysis is an interpretation of international law. Just like domestic courts have to interpret domestic law, the Tallinn manual process interprets international law. It means that the lines are not very clear, but these are the lines were drawn by twenty international law scholars. Some of the thresholds discussed during the Tallinn Manual 1.0 process were:

Physical Presence in Territory – When you have organs of one state (such as an intelligence organization) in the territory of another state conducting cyber operations in that territory, then that is a violation of the target state's sovereignty. We have kinetic analogies. When Russian military aircraft penetrate Estonia, Swedish, or Finnish airspace for a few seconds, most will say that is not an armed attack. However, that is not lawful under international law. It is, instead, a violation of sovereignty. When you have Russian intelligence agents coming across the Estonian border and actually capturing an Estonian intelligence official, then taking him back to Russia, that is not an armed attack but another example of a violation of a state's sovereignty. The other state did not consent to this "organ of the state" actions. It is a violation of international law.

Remote Physical Destruction or Injury – This is more complex when talking about remote cyber operations, such as the U.S. engaging in cyber operations in another state without being physically present in that state. The first situation was that if the remote cyber operation causes physical consequences in the target states, then then this is the same as the acting state is physically present in the target state. Stuxnet was a perfect example of a state actor (allegedly conducted by Israel and/or U.S.) violating another state's sovereignty. Most cyber operations do not rise to this level either.

Remote Loss of Functionality – What about cyber operations that cause less than physical damage from remote cyber operations, such as the Saudi Aramco attacks where thousands of computers stopped working due to Shamoon malware attacks? Saudi Aramco's computers were physically attacked and destroyed (and they had to be replaced). This was considered a violation of Saudi Arabia's sovereignty, a type of cyber operation that was a violation of sovereignty based on "the loss of functionality." If you knock out cyber infrastructure such that is has to be replaced, that is a violation of sovereignty. Next question members addressed involved lesser damage, such as if a state had to reinstall operating systems or reinstall other software after cyber operations – is this a violation of sovereignty? That is where they members started to split.

Remotely Operating Inside Cyber Infrastructure – What if you are just remotely operating insider a cyber infrastructure of another state and instead of trading data you are installing back doors? There are some that say that what you do inside those systems is the same as you are physically present in that state territory, but most international lawyers will not take the legal analysis this far. This was considered be an unacceptable result for states by rendering all aspects of cyber espionage unlawful, which does not make sense with today's reality.

In the Tallinn 2.0 Manual process, an additional threshold discussed was the Usurpation of Inherently Governmental Functions. Members could imagine a state manipulating the election results of another state or interfering with tax collection via cyber means in another state. These types of cyber operations can have such severe consequences and just taking the physical analysis forward step by step, that this would qualify as physical presence in another state's territory. Our members started thinking what sovereignty means, and came back to the 1928 definition of sovereignty, that it is the right of a state in sovereign territory to exercise the functions of a state. If a cyber operation usurps inherently government functions of another state, such as discussed above, and it puts in power a person not elected, it is a usurpation of a government function and that this act is a violation of sovereignty, in other words, an unlawful act under international law.

**Freedom of Expression, Right to Privacy, and Sovereignty in Cyberspace**

If two nations or two jurisdictions have the exact same legal values or the same expectations for cyberspace, then the sovereignty issue should not be as difficult to figure out with the lack of geographic borders. Why would cyber sovereignty matter?

Every jurisdiction has its own values inherent in both its law and approach to cyberspace. The issue becomes when you have two different nations or two different jurisdictions with two different legal regimes…how do your permanence that? When looking at the U.S. and China, it is obvious U.S. has very different values, very different legal values, and views different views on human rights (and cyber) than China. To show the real difficulty of sovereignty in cyberspace, it might be more prudent to talk about the views of cyberspace and legal rights of both the U.S. and European Union. Obviously we are much more allied, with human rights much more central to both of our approaches.

But there are significant differences. In the U.S., freedom of expression is going to often be more important than privacy on the Internet for a lot of policy makers and the courts. In the European Union, privacy is often more valued than freedom of expression. Not stating what is right or wrong, but there are significant differences in approaches.

In a law review article written by Samuel Warren and Louis Brandeis in 1890, The Right to Privacy, both were concerned with what they saw as gossip in the news media (i.e., Yellow Journalism) with rumors that they were invading privacy. The article was important is that they helped create common law torts, the causes of actions one can pursue for privacy violations. What is also important is that this started from a real concern on how people were expressing themselves. So even back then, there was a tension between free speech and privacy.

In the U.S. Constitution, Freedom of Speech is a fundamental right of its citizens under the First Amendment. In the U.S., Congress shall make no law preventing one's freedom of speech (although the since carved out some minor exceptions). Within the U.S. there is a strong, absolute view of freedom of expression being supreme. Some ways the U.S. has bounded freedom of expression include:

- Defamation Law: It is darn near impossible to bring a defamation lawsuit in the U.S. You can but you really have to have something really bad thing happen to you and have a great lawyer. This is not the case in the U.K., where it is a whole lot easier.
- Section 230 of the Communications Decency Act: This goes to Congress and this law is important in that it stated that with some exceptions of intellectual property and federal criminal law violations, other than those exceptions, you cannot hold a social media website or ISP liable for the content provided by its users. Fairly simple law. If we did not have Section 230, we would not have Facebook or Twitter. Could you imagine if they were responsible? You would have a very conscious, edited environment and Internet (as we know it today) would not exist.
- Citizens United: Citizens United is an organization that used the First Amendment to loosen and eliminate restrictions on campaign finance spending.
- U.S vs Stevens: Mr. Stevens was convicted under 18 U.S.C. Section 48 in a Pennsylvania federal district court for "knowingly selling depictions of animal cruelty with the intention of placing those depictions in interstate commerce for commercial gain." A U.S. Court of Appeals agreed with Mr. Stevens and reversed his conviction, holding unconstitutional 18 U.S.C. Section 48. The court reasoned that the dog fighting videos he sold were protected speech and that 18 U.S.C. Section 48 did not serve a compelling governmental interest.
- Failed attempts by the U.S. at regulating social media in terrorist prevention efforts.

Within the European Union (European Convention on Humans), there are notable differences between E.U. than U.S. views on Privacy and Freedom of Expression.

Privacy: In Article 8, privacy is pretty straight forward (similar to what our First Amendment says about freedom of expression). Everyone in the E.U. has the right to respect for his private and family life, his home, and his correspondence.

Freedom of Expression: In Article 10, everyone has the right to freedom of expression, with some limitations and conditions. This article does reflect E.U. values that privacy is a fundamental human right, and that freedom of expression is important, but privacy is afforded a much greater weight in the E.U. than the U.S.

Privacy and the Right to be Forgotten: Within European Privacy Law, Privacy is considered a fundamental human right. In 2010, an Italian Court made a criminal ruling against Google executives for failing to prevent the posting of a video of a boy being bullied. In the U.S., you would not see that happening, and without focusing on the right or wrong, most of us would see executives going to prisons over user content as chilling. Additionally, within the E.U., Europeans have the right to be forgotten, specifically that under certain circumstance, to ask search engines to remove links with personal information about them where the information is inaccurate, irrelevant, or excessive for the purposes of the data processing. This is not an absolute, but will always need to be balanced against other fundamental rights such as the freedom of expression and of the media.

Even amongst allies, it is hard to find common ground on the more important issues in cyberspace. So when we talk about sovereignty, you have to look at how you respect the other jurisdictions, and this will be hard. Imagine other jurisdictions where there are wider differences.

**DOE Cybersecurity Coordination (U.S. and Canada Grid Cooperation) and Information Sharing**

The Department of Energy (DOE) is a complex enterprise with a wide range of missions ranging from basic science to nuclear security and beyond, and evolved into a broad range of things from energy efficiency rating on your refrigerator to making, storing, and sharing nuclear weapons for military. The DOE mission is "to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions." The DOE is the 14th largest agency by size, and has entities (organizational components) in twenty-seven (27) states employing more than 108,000 people, about 14,000 of which as federal government and support service contractors, and 93,000 are Management & Operating (M&O) and other contractors.

One crucial mission at DOE is leading federal efforts to enhance the reliability, security, and resilience of our networks, and much of this is accomplished in DOE National Laboratories. The bulk of DOE employees (93,000) are managed and operated. DOE owns the national laboratories, but contracts out the work so things get done faster because you have a little less of government on top of everything that is going on. There are 17 national laboratories that are home to some of the most powerful lasers, fastest computers, and Nobel Prize researchers. Our national laboratories came about when the U.S decided to out-innovate our enemies prior to and during WWII. We are the home of the Manhattan Project, and our national labs are where our most advanced U.S. weapons come from.

In a recent conference focused on "Cybersecurity and Grid Cooperation," the Under Secretary of Homeland Security for National Protection and Programs discussed how our energy grid is not unique to the U.S., and that it was shared with Canada and to a lesser extent, Mexico (Baja). In trying to enforce cyber security standards in the energy grid domestically, it appeared that our model would not work if this was done in Canada. While we can use the Federal Energy Regulation Commission (FERC) as the regulation body for the energy industry to enforce cyber standards in the U.S., FERC cannot tell Canada what to do. Ms. Spaulding was asked how the U.S. could make this work, and respect Canada's sovereignty, at the same time to keep us safe as there is no imaginary wall between Canada and the U.S. when it comes to the energy grid. Canadian vulnerability is U.S. vulnerability, and U.S. vulnerability is Canadian vulnerability. She stated that when FERC comes out with a cybersecurity standard, the U.S. has a relationship with Canada that is very friendly and unique internationally. The U.S. cannot go to Canada at the Federal Level, but they can go provincially, and province by province we can explain the FERC standard, what it means and why it was put out. When Canadians get this understanding from us, they adopt FERC standards voluntarily. So in this instance, the U.S. confirmed that they respect Canada's sovereignty. The U.S. does not tell Canada what to do, but the U.S. was able to get to a level of common security effect. This is accomplished because U.S. agencies like DHS and DOE have spent many years building relationships with their Canadian counterparts, and it is based on trust and mutual shared interests. The U.S. would not be able to achieve success if they told Canada what to do without any legal basis.

The DOE is committed to sharing information between the government and the private sector. Under Presidential Policy Directive 21 (PPD 21), DOE has been designated as the energy sector specific agency, and is responsible for working with energy companies to help develop a stronger, safer, and more resilient power grid. The Cyber Risk Information Sharing Program (CRISP) is now in its third year of operations, highlighting DOE's commitment to helping ensure a more reliable flow of energy in the U.S. In the simplest terms, CRISP allows energy companies to voluntarily share data with the North American Electric Reliability Corporation (NERC), via their Electricity Information Sharing and Analysis Center (E-ISAC). The NERC's E-ISAC then shares this information with other U.S. government agencies. Thus the sharing of this critical information is not managed not by the government, but instead by the E-ISAC (the industry group). The shared data is then analyzed by the government for threats, and when DOE gets this information, DOE brings this down to the unclassified level and then shares it back with the energy sector. There are an estimated 3,000+ energy companies out there, although there are not 3,000 members of CRISP. However, once DOE anonymizes this information, it can share it with CRISP participants, and then with the industry. Unlike FERC, the DOE is not a regulator in the energy sector, and CRISP is an entirely voluntary program. CRISP is mentioned on both the DOE and NERC E-ISAC websites – the only classified information we have are the sources and methods used to identity the threats.

Regarding the legal dimension of CRISP, strict privacy and civil liberties concerns have been baked into the program. DOE decided to be extremely conscientious about privacy and civil liberties in building CRISP, covering very specific requirements based on the Fourth Amendment. When CRISP users go to use a CRISP-covered computer, there is a log on banner requirement. Users cannot access a CRISP-covered computer without consent via a log on banner. For those who are covered by CRISP, there are three main things DOE requires of companies if they are to participate in CRISP. DOE has actually turned down major companies who have refused to do this because we care that the DOE and the USG are not perceived as violating the 4th Amendment.

- Expectation of privacy – when you use a CRISP governed computer, the banners must tell you that you have no expectation of privacy when you are using a CRISP governed computer.
- Consent to sharing information that is transiting or stored on the computer you are using (told up front that whatever you are entering into this computer can be shared).
- Giving notice up front that the information transiting on the computer, to include information you put on it, can be shared with the government

Therefore, every computer covered by CRISP must have this banner on it, or it is not meant to be a part of our program.

In addition to the above, DOE takes it one step farther. Besides addressing the privacy and civil liberties concerns using log on banners, DOE wants to make sure there is no misunderstanding for employees of these companies. DOE baked in a yearly training requirement, so that when companies give their employees yearly training, they are required to give training on the banner. There is no confusion therefore on what this means.

Even with these stringent requirements in place, DOE has been able to attract significant industry participation. CRISP has more than twenty volunteers from the energy sector, are these are not small companies (they cover an estimated 60% percent of energy customers in the U.S.). CRISP is a real program, sharing information back and forth between the government and private sector. It represents one the largest and most successful public-private cyber threat information sharing programs ever built. Through CRISP, the energy industry is much better able to see cyber threats that we face today, and that we continue to face in the future. CRISP allows for crucial cyber-threat information sharing to occur between companies that are oftentimes competing against each other. This is really important for a successful information sharing program. It also helps DOE fulfill its responsibilities as the energy sector specific agency under PPD 21, and it also helps provide us with situational awareness of our own networks because it would be naïve to think an attack on the energy grid is limited to only the energy grid. Next step for CRISP involves securing SCADA. Not going to happen tomorrow, but we are absolutely aware of the problem and we are trying to address it.

**Ethical Cyber Warfare (Just War Theory)**

In looking at different conceptual questions from a philosophical point of view, we need to look at cyber sovereignty and how does cyber warfare play out in the ethical realm and not just the legal realm.

There are two prevailing perspectives when discussing cyber sovereignty and warfare from a philosophical, ethical perspective. The first perspective involves “jus ad bellum,” the right to go to war, and “jus in bello,” the right conduct in war. In looking at the ethics of war, and traditional Just War theory questions, we need to investigate how those apply to cyber war if they do at all. Many people think they do not, while many others contend they do. In addressing Just War theory from a cyber warfare context, we specifically need to look into the question of harm itself – the harm to civilians across state-to-state lines as well as state-on-state cyber warfare actions and with non-state actors.

The traditional lynchpin of Just War theory is civilian immunity from harm. This does not mean civilians can’t get hurt in war, as they often sadly are. But it means that traditionally in Just War theory, for any jus in bello criteria, you need to not intentionally harm civilians. It also means that civilians cannot be used to achieve a particular end. There is a doctrine of double effect that works through a series of questions you can work through on both intentions and means for unintended harm to see who really is a side effect or not and morally justified.

The question, or puzzle in all of this, is how do certain kinds of harms aggregate in certain ways or whether or not they do at all to reach certain thresholds that we think could justify a lethal response. In an extreme case, justify something like war, under jus ad bellum. Philosophers have danced around with these fanciful thought experiments and weird questions about how these things play themselves out, and then along came cyber warfare. Cyber provides an intriguing real world example of these aggregation puzzles, and what harm actually plays itself out.

A first question involves at what point does aggregated harm rise to a level where it would trigger or justify some violent, legal defense – this gives us an analog for a lot of cyber war operations when it comes to civilian immunity from harm. Civilians are truly immune from harm in Just War theory, both from being intentionally harmed or as being used as a means to an end during a specific military operation. It seems like it is going to push up against a lot of cyber warfare operations, because a great deal of cyber warfare operations will indeed use civilian infrastructure and civilian cyber networks of all types to at least carry the weapons of war, as well as being used to coopt cyber infrastructure.

You might say it does not matter, or that is does not hurt or harm them, so there is no harm, and that it is using them and thus cannot constitute a violation of civilian immunity. The Tallinn Manual has a lot of limitations on this matter, as the Tallinn Manual and International Committee of the Red Cross (ICRC) are going to look more at International Humanitarian law over relevant thresholds like death, injury, destruction of property, loss of functionality…but that really does not capture the puzzle here. Here is the puzzle (and there is a great divide in philosophy over this) – do certain kinds of harms themselves aggregate themselves up to justify certain responses? Or cannot they be aggregated? This is the division in normative theory between consequentialists and non-consequentialists.

For consequentialists, taking a utilitarianism viewpoint, you just add up any number or harms on one side of the scale, and if it tips over a certain threshold you think it is justifiable to use a certain type of response, you can justify your response to somebody. For example, if I flick an ear of someone, once a day, it would not be enough of a wrong for him to justify him killing me. It would not be a proportional response. What if I flick his ear 1,000 times, or 1,000 times a day for 10 years? Eventually that could aggregate up enough (meets the condition of necessity), and that the only to stop this was to kill me, then perhaps it would be justifiable and maybe even proportional. Does this type of harm aggregate in such a way that justifies a violate response?

For non-consequentialists, they would say no. They state that certain kinds of harm (serious bodily injury or death or destruction of things) are the only thing that can justify proportional responses of violence.

The problem in the cyber world is exactly the kinds of things we have in the puzzle before us. Imagine a cyber weapon that is going to use civilian infrastructure and all that it is going to do slow down the computers temporarily, e.g., slow down one's access to email, one would clearly think that this is not something proportionately to justify the response of war. However, what if it involves thousands of people or millions of computers? At what point then does harm of this kind to civilians (with minor harms) aggregate to major harms, or don't we think these kinds of harms aggregate in these kinds of ways that you actually do need true destruction or true loss of life? These are some puzzles of harm that philosophers have questioned for years in defense of harm, but now we are a point where we need to answer this question that builds off the nature of harm in order to understand how we think cyber warfare can be justly played out in the international realm if we think civilian immunity from harm is an important lynchpin in Just War theory. Notice the jus ad bellum side of this, the justification for going to war, is going to impact our intuitions in jus in bello side, how we behave in war.

In the cyber war realm, we need to be definitively clear on what we think constitutes harm, and whether or not we think that harm can be aggregated. If we answer yes, that any sort of use of civilian infrastructure or systems is a kind of harm, and we do think those can be aggregated, then the surprising upshot is going to be that most cyber warfare is going to be difficult to justify under traditional Just War theory methods.

There are many that would envision cyber warfare as a potential moral improvement over other forms of warfare, precisely because the harms that cyber warfare can bring about are often non-lethal and much more discriminant and much more carefully proportionate to the cause they are trying to carry out. However, if along the way, if a significant number of civilians are harmed in the process, even if minor, we have a problem in jus in bello civilian immunity that we have to figure out.

### Restoring Trust Between the U.S. Government and Private Sector

The Electronic Frontier Foundation (EFF) is a civil liberties organization dedicated to defending civil rights and liberties in a digital world. EFF clients include those who have hacked voting machines, ATMs, airplanes, cars, medical devices, safes, access cards, cell networks, alarm systems, and IOS passcode locks. EFF clients include professors at major universities, high school students in their parent's basements, hackers at defense contractors in Northern VA, and companies that include TELCOs, Internet Communications Providers, and ISPs, you name. EFF also conducts national and international litigation, to include the government of Ethiopia, Kazakhstan, and U.S.

First, there is a problem in defending U.S. sovereignty on the Internet in the cyber domain. We don't live in the days of ARPANET, those days are over, and the Internet is not ours anymore. The Internet is a thing that exists well beyond any one government's reach. This presents problems. There are things like the signal protocol and communications. The founder of EFF, John Gilmore, stated in 1993 that "the net interprets censorship as damage and routes around it." At that time, there were no things such as a VPN (in practice), and TOR was not a glimmer in even the Navy's eyes.

> *Note: The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.*

The Tor project is based on the belief that anonymity is not just a good idea some of the time — it is a requirement for a free and functioning society. The EFF continues to stress that anonymity was crucial to the founding of the United States, and that anonymity is recognized by US courts as a fundamental and important right. In fact, governments mandate anonymity in many cases themselves, such as police tip lines, adoption services, police officer identities, and so forth.

It is clear that the Internet has drastically changed the way in how we all communicate. We are all free to post pictures of our cats to send to Nigerian scam emails, use cryptography, and we can do it from anonymous locations. This poses major problems. This came to a head after Jung revolutions in 2013, when a company sued a small ISP and its owner for distributing free software. Since then, Silicon Valley by and large stopped cooperating – they just don't anymore.

In 2010-11, Google suffered a major breach by the Chinese, who breached Google's law enforcement access portal. Google at that time was able to turn over the content of its email to the U.S. government when presented a warrant for probable cause or other circumstances. What was disconcerting was that Google was also turning over that content to the Chinese at the same time without knowledge. When that happened, Google allegedly called appropriate U.S. Government organizations, and the U.S. Government helped Google in backing the Chinese out of its networks and helped them get better. Does anyone here think that Google today would actually depend on the U.S. Government for that kind of assistance? Maybe, but they certainly would not do it like they did then.

Apple is another key, recent example. Besides the majorly ignorant description of that conflict, it was a major conflict and Apple simply did not cooperate. That is a problem for everyone. That is a problem for the U.S. Government, DoD, Intelligence Community, Law Enforcement, and companies. This needs to be fixed now. We need to highlight how especially broken this is and find some ways to fix that in a way that the U.S. will regain the ability to defend its sovereignty in the Cyber Domain.

The Vulnerability Equities Process (VEP) was drafted in 2010-11 as part of a multi-agency process where the U.S. government figures out what to do when it becomes aware of a vulnerability in a system that does not belong to the U.S. Government. It could be Googles' law enforcement access portal, or it could be IOS passcode locks, you name it. VEP just sat there after being signed, almost unimplemented and almost unused until 2014. The current White House Cyber Czar reinvigorated the VEP, and VEP was functioning for a brief time in 2014. Then it broke again, in large part due the Apple fiasco that saw the FBI buying a vulnerability from a party that was widely purported to be Celebrate. Somewhat disconcerting is that the vulnerability was acquired in such a way that the FBI officially never learned of the details so it did not have to put it into VEP.

When EFF asked several individuals/officials in Google working security regarding the number of vulnerability reports have they received from the U.S. Government, the answer being none to their knowledge. Google is not aware, as an institution, of any vulnerability reporting from the U.S., despite all the claims to the contrary on how well they are sharing vulnerability information. So when we see things such as the VEP being reinvigorated, and then we what happened in San Bernardino, and we see Silicon Valley's perception of the VEP, there is a massive disconnect. Needs to be fixed.

The U.S. Government seems to have a fetish with classifying things. The New York Times in 2005 had a front page story that broke the news of Stellar wind. The U.S. Government could neither confirm nor deny the existence of this program until years later, nearly a decade after it was front page in the New York Times. The VEP is public only because of a FOIA lawsuit under a colleague at EFF. When EFF first filed its FOIA request for VEP, they got a Glomar response "neither confirm or deny." The U.S. Government backed off of Glomar very quickly, and then released a highly redacted version, which was further then redacted to eventually coming down to only a few redacted things. This does nothing to help give Silicon Valley assurance that the government is on the right side.

It was recently announced in the news and social media that the SIGINT and IAD within CYBERCOM were being consolidated. That makes perfect sense from an operational standpoint, as you cannot practice defense without knowing offense just as well. If you are not practicing offensive skills, I do not want you to be defending my networks or this country. But the decision to combine SIGINT with IAD did not fly well in Silicon Valley. Going back to the Google example – why on earth would Google now invite IAD into their network to help them secure them from the Chinese if the same people were people were responsible for SIGINT? There might be good reasons to do this, but that does not matter to people at Google, Facebook, Twitter, or Apple. They are not Intelligence Community people, they do not care about the SIGINT mission, all they care about is IAD. They are not going to give access if they think that their trust is going to be exploited by the same people who they have invited into secure their networks in the wake of combined IAD and SIGINT.

Finally, there is the issue around "Trickle Down." The capabilities, techniques, exploits, and tools that the people in this room developed and/or use to protect us in the cyber domain to wage cyber war and exercise Title 10 powers have and will continue to fall very quickly into the hands of state and local law enforcement. For example, IMSI Catchers were developed and deployed for SIGINT in the Middle East and other operational theaters by DOD components. Within a period of months and years, they were now in the hands of the FBI and very quickly State and Local Law Enforcement. It was almost a decade before courts were told that IMSI catchers were being used in these instances. The tools you develop and deploy will not stay in the cyber war domain. It is not going to stay in the hands of DoD personnel being used overseas, they will fall to state and local law enforcement entities. There is a well-known publicized prosecution going on involving thousands of people who accessed a terrible child porn site called Playpen. The exploit that the FBI used to find the people accessing this site used a classified technique, and since it used a classified technique, it could not be disclosed to the defense counsel. Because since it cannot be disclosed to the defense counsel, thousands of court cases as we speak are falling apart, and thousands of child predators will soon likely be free. So when you are developing these tools, and know they are going to be used here by domestic law enforcement, and you have got to figure out a process of doing that better.

In the private sector, the reason many of us trust private actors to collect so much data about us is this theory of notice and consent. The reason that CRISP works is because of notice and consent. In the government context, it is a little bit different. I am talking more about the Intelligence Community than the DoD. We need to figure how to get back on that track. We need to figure how something can be on the front page on NY Times News for ten years but yet still classified, and start holding people accountable. We need to have judges in areas in Washington D.C. other than a SCIF, which is where the FISA Court meets, actually passing on the legality of some of these techniques. So we need transparency and accountability. Until we get both of those things, we are not going to get the trust of Silicon Valley.

> *Note: According to the EFF, the Foreign Intelligence Surveillance Act (FISA) Court is no longer serving its constitutional function of providing a check on the executive branch's ability to obtain Americans' private communications. Dramatic shifts in technology and law have changed the role of the FISA Court since its creation in 1978 — from reviewing government applications to collect communications in specific cases, to issuing blanket approvals of sweeping data collection programs affecting millions of Americans. Under today's foreign intelligence surveillance system, the government's ability to collect information about ordinary Americans' lives has increased exponentially while judicial oversight has been reduced to near-nothingness. The role of today's FISA Court no longer comports with constitutional requirements, including the strictures of Article III and the Fourth Amendment.*

### Deterrence in Cyberspace

In the DoD Cyber Strategy, the Secretary of Defense stated that "deterrence is a key element" of our cyber planning and strategy. So what does it mean when we talk about deterring our adversaries, and how many of you think there is a level playing field between us, China, and Russia? In order for the U.S. to hold states accountable under this wonderful international system that a previous colleague has explained, states have to play by the rules. They have to sign up to these rules, and they have to enforce them internally and externally. The problem we have is that there are asymmetric elements to this contest. When we talk about nationalist hackers and hacker militias in China and Russia, how many of you think those are not under control of their respective governments?

How many think the U.S. government controls every hacker in the United States? That is the point, we do have law enforcement but we don't have control. So when we talk about the activities of different states, you cannot just apply the international system as if everyone was observing that. We instead have to apply as reality actually exists on the ground or cyberspace. You have to look at what is the level of control or direction from the sponsoring state, with sovereignty and responses to sovereignty being state-to-state issues. Obviously, those states who have control over their external hacking activities, we should hold them responsible for that level of control. Indeed, the Tallinn Manual describes the process on how we do that. Conversely, in those states that are so weak (like Somalia and Afghanistan) that have no internal controls, we may have to have to engage externally to protect ourselves.

Our nation is doing this backwards. We are taking a wonderful international system designed on kinetic effects in warfare, and trying to overlay it over an amorphous and trans-jurisdictional set of conflicts. One could argue that the U.S. should do it in reverse. We should have our experts from multiple DoD and U.S. Government identify those activities which individually or in the aggregate represent a threat to this country. From an ethical point of view, we can aggregate them in different ways. However, most of us can agree that a series of aggregated steps which resulted in some external force gaining control over the launch codes of our ICBMs – that to me is an act of war and should treat it as such. That means we should identify those activities (individually or in the aggregate) that are unacceptable to this country and its security, and we should make them illegal. The second part of that is signaling this to the rest of the international community that we will not tolerate that. I think it is within the framework of the Tallinn Manual to say that certain activities are violation of law. Then the question is, okay, what are you going to do about it? We have to enable and support our cyber components, our response teams, and all of the other machinery that we have to take responsive action when we have to do it. If we don't do it, we allow other governments in an asymmetric playing field to take over and undermine all of our critical infrastructure. We will find out that international law has indeed changed, because some people are going to be passive victims and some people will be active aggressors. That is not how international law should work, and we should not allow it to work that way. So I would argue that unless we clearly identify those activities that we will not tolerate, and unless we put the international community on notice that we will take action, and unless we thereafter do take action, we will simply become a suicide victim of international law.

The National Guard and Reserves now form a significant portion of our Cyber Response Teams. That is important as Guard and Reserves have all these civilian activities, i.e., they work at Google and Microsoft and leading-edge cyber companies, and they bring a lot of intelligence and creativity to the process. They need to be part of the team. How many of you think that those teams between Guards, Reserves, and Active Duty are interoperable? They are not interoperable because of a plethora of rules inherited from the founding of the country talking about state sovereignty. State sovereignty amongst all of the states and territories is great for many things, but it does not work in Cyber. We need to serious consider it as a matter of policy and regulation that we change the law to enable Guard, Reserve, and Active Duty Cyber Units to operate seamlessly, to train the same way, and to be plug and play the way we the Army does with its Brigade Combat Teams (BCTs). I believe it is time we created a credible and fully operational national force.

As for cyber militias, there is something to be said on revisiting how we do business, and I would argue that we should now enlist and employ the most unconventional people we can find, because that is the nature of this threat and this activity. We should go out and actually recruit, and find ways to accommodate within our national security system those wonderful, brilliant, unconventional minds. They may not be qualified in PT or in firing weapons, but they are very good at what they do. To give you an example, Einstein was not allowed to work on the Manhattan Project because he could not get a security clearance. He was considered a problem. We need now to find statutory and regulatory ways to allow the most creative and unconventional people to be part of our Cyber National Force. We should not be restricted by inter-service rivalries or inter-service traditions or all these wonderful things…yes they have a great place and for the trigger pullers on the ground, it makes sense. With this new type of warfighting, cyberwarfare, we need everybody. Let's follow the example of the Bletchley Park codebreakers that broke Enigma. While they were actively recruited and needed, they would never have been welcomed into the Army. We should stop fooling around and tip toeing around the old international norms, and we should take charge and define what it is that we as a nation will not tolerate to our security and infrastructure. We need to put people on notice, deter them, and respond when they are not deterred. We need to enlist and employ all these wonderful people in the U.S. that will enable us to do that.

### Rules of Engagement for Cyber Warfare (On the High Seas and International Environments)

Within the cyber realm, the civilian or non-combatant distinction is not as applicable in Just War theory. For example, in World War II, there were sinking of civilian ships. There are clauses in international humanitarian law for military use of civilian infrastructure, but most of the times that would be a blatant disregard of the combatant and non-combatant distinction. China's hacking of Google is direct targeting of a civilian company, and that would be war crime if you think it is cyber warfare. We don't seem to treat it that way in the cyber realm, as we don't seem to treat cyber engagements on civilian assets versus military assets as if it were a bomb. If a rocket hit Google, there would be no debate and it would be a war crime because it is directly targeting civilians. In the cyber realm, we seem to blur the two distinctions.

It also depends if you are in armed conflict or not. If there is an armed conflict on the high seas, then the law of war or the law of armed conflict would apply. You will likely not just see cyber only in an armed conflict, it will most likely be cyber plus kinetic. Then we could apply the same rules as you would apply to non-cyber armed conflict on the seas. But when you talk about cyber operations against other states vessels during peacetime on the high seas, then military vessels enjoy sovereign immunity, which means that you cannot engage in cyber against that foreign vessel. It is not territorial sovereignty that you apply in that context, but it's a derivative of territorial sovereignty with sovereign immunity that state owned vessels and military ships and aircraft enjoy, but not commercial vessels.

### Establishing International Norms on Protection of Intellectual Property

Is there a way for the U.S. or another nation to establish international norms on the protection of intellectual property? Today, no. The U.S. and other nations have made attempts to do so with various trade negotiations, to include the TPP which has become a big issue of Presidential campaign. When big companies in the U.S. talk about intellectual property, 90% of time they are talking about China, and China won't participate in that. They may get lip service, but nothing else.

## Evolving Threats and Challenges

*BG Maria Barrett, Deputy Commanding General for the Joint Force Headquarters, ARCYBER*

During this presentation, our distinguished guest speaker discussed the evolving cyber threat, and some challenges and opportunities to counter this threat.

**Evolving Cyber Threats**

Over the past decade, the threats in cyberspace have grown since then and continue to grow in scope, scale and reach. We need to only look at a few specific incidents to confirm this position – Chinese military hacking into Pentagon computer networks, Russia's intrusion into the Ukraine's Power System, and North Korea's hacking and destruction of property at Sony. We most recently have reports of an Iranian attack on a New York dam, and violent extremist organizations like ISIL using of cyberspace to recruit and control the regional narrative. The trend is not good, continue to see this activity increase from both state and non-state actors.

As the world's reliance on cyberspace grows and the number of devices that are and will be connected to the Internet today which will grow to an estimated 50 billion by 2020, these malicious cyber actors are targeting both government and private industry. So within the Cyber National Mission Force (CNMF), our focus is on those malicious cyber actors that cause a threat to our national interests. While these threats come primarily from nation states (Russia, China, NK and Iran), we continue to look at any trend that involves non-state actors developing capabilities in cyberspace that impact our national interests. These actors are moving on a very disturbing trajectory from exploitation to disruption to destruction. Along the exploitation lines, state and non-state actors are stealing information or doing reconnaissance, so I would put the intrusion into the Joint Staff Network within this category.

There is a growing concern on the large amount of data repositories we have, which in turn has implications from a Personal Identifiable Information (PII) aspect. A few years ago most average companies and organizations could not process and securely store all of its data. With the advent of data analytics, even if we cannot get to analyze it all, this has made it possible to make all of this information useful and therefore we have become a bunch of data hoarders. This data tool is a tool for both business and the government, but it also has become a target such as was the case with Health Insurer, Anthem, has found out when hackers broke into their database(s) containing personal information on about 78 million people. Anthem said hackers broke into a database containing personal information ...what is likely to be the largest data breach disclosed by a health-care company. You have got to take a look at your constituency, whether you are in the DoD or if you are a business, and take a lot a look at this threat (data repositories are both an asset that enables you to do this while it also makes you vulnerable at the same time).

While denial of service attacks has been the mainstay of disruptive attacks, there has been a significantly increased use of ransomware to extort companies that is particularly troubling as well.

Lastly, on the destructive end of things, there is an increasing willingness by our adversaries to use disruptive attacks such as North Korea's attack on Sony, recent attackers who stole $80 million from the Bangladesh central bank by hacking into software from the SWIFT financial platform, and Russian attacks on the Ukrainian power system. What made Russia's attack unique was the way in that they did it. It was their use of electronic warfare, information operations, and a cyber attack to achieve a tactical, operational, and strategic end.

**Countering the Threat – Challenges and Opportunities**

In looking into what our nation and armed forces need to do with these threats, we have to defend our networks. Until recently for both the public and private sector, cybersecurity has been focused on our computer platform and our networks. Many of us realize that when we put computers into our vehicles, power plants and warfighting platforms, and then connect them, these platforms become vulnerable to the same threats our networks faced. The same technologies that worked for us and made us cutting edge over last couple of decades are now significantly changing the world around us, and are creating asymmetries which disrupt our operational environment. We need to take a look at this, as this creates opportunities for us as well.

While we are not finding many Cyber Cities in Syria and Iraq, this is certainly something we have to take a look at and fold into our repertoire if we are going to do cyber. This is a cyber environment that our Commanders are going to be operating in for some time. While it seems very obvious that we need to design for cybersecurity at the start (during specification and design of these systems) and need to stay ahead, we have to be able to develop things (technologies, systems, and platforms) which we can defend from attack. We talk about isolating systems and weapons through possible islanding, but something else is needed that enables us to be more resilient and be able to fight through attack. Pencils and acetate are actually coming back into our discussions, it is one way to achieve resiliency, and reflects our thinking on how to work through a contested environment. Again, it would be helpful if we did this at the beginning of the design phase. This does require cooperation across the entire cybersecurity life cycle (from basic industry and academia research) and venture capitalism, and then government signing this provenance. This approach still requires that we put protection on things in cyberspace that makes attacking these systems more difficult, more time consuming, and most costly for the hacker. At the end of the day, our goal is mission assurance, to the extent to which we can make our networks more resilient.

We also need to ensure we provide full spectrum capabilities for our warfighters and the policy makers. We need a variety of options for them to choose from, and these options need to be well understood. This is a difficult field and it been ruled that it is hard for some folks to wrap their head around, what the option we propose actually does, and from a legal aspect up to the effects aspect. The cost calculus needs to be changed, and we need more difficult for those attacking us. We want to make adversaries think about blow-back from them attacking us, getting to the deterrence aspect of this subject. On the battlefield, tactical innovations like the cyber capability rifle will mean nothing if commanders and planners do not know to integrate these effects. Planners should consider integrating cyber with non-kinetic capabilities such as information operations, electronic warfare, and space. The effects a Commander wants to achieve does not necessarily have to combine all these things, but in a lot of cases they will find there is a very good fit. Commanders will find that they can use cyber to shape the environment, or in direct support of a maneuver warfare, just like another instrument of war. Above all, Commanders operating in this environment will recognize the terms and principles found in maneuver warfare are applicable – targeting, critical vulnerabilities, collateral effects, operational tempo, combined arms, surprise, adaptiveness…all of these are applicable. There may not be a complete analogy in this sphere (which can go terribly wrong), but if you do think through these tenets they are true, and it is incumbent upon us as planners and commanders to think about how the cyber effects were planning achieve these type of effects. So whether it is defending the DODIN, or the Internet in which our nation's critical infrastructure depends, these terms are applicable. From a defender's perspective, there is the concept of "defense has maneuvers." We finally are starting to get that message. We are probably not where we need to be in combining intelligence with planning with the security of our systems, there is still more work in that space.

We also need to ensure we have a framework for defending our nation in executing cyber operations, not just across the DoD, but to make sure there is a bridge to the entire U.S. Government and the private sector on how to address threats in cyberspace in an integrated and national way. Why, because at the base of the elements of national power, diplomatic, informational, military, and economic – military is but one aspect. So this does not need to a cyber versus cyber proposition – it needs to be considered with all the other elements of national power. Not sure we have all those bridges in place to smoothly do that. You will get there by doing this over and over again, we just have not built up that muscle memory yet.

We also need to recognize the source of innovation has changed. Government was once the primary source of innovation for war, and now industry is the leader in information technology and cyber security innovation. Those that are critical on how we deploy and bring to bear new technology in this space are right to be frustrated. We talk about big companies versus little companies, and in nine months at CYBERCOM have definitely seen examples of how we do not want to continue doing it. Whether it is something we have found in private industry, or it is something that our teams have developed, we are finding that it still takes months to bring that to deployment. Making the process shorter key priority. CYBERCOM's public-private partnership in Silicon Valley, the DIUx, is an investment involving partnerships with the research community that will go a long way in addressing cybersecurity at the front end of the equation in offering the technical and intellectual innovation that we need to partner with our expertise in the age of cyber warfare. We need to also recognize the value of threat intelligence and information sharing in this sphere, as every sector of government, especially military and law enforcement, sector specific industries, and the security industry all have key insights into achieving security. This does not happen by accident, and some of this is hard. Comprehensive exercises such as Cyber Flag and Cyber Guard gives us the ability to ferret out some of the issues related to this and working on them, but we need to work on them a whole lot faster.

There is some debate that the culture of cybersecurity is not consistent across DoD, but this may be in large part that every organization may not be properly resourced. Some are better than others, and this will always be an uphill battle.

CYBERCOM JTF Ares was created to develop and use state of the art cyber weapons that can damage and destroy the Islamic State's networks, computers, and cellphones under JTF Ares. This is but one of the capabilities the DoD is bringing to the fight.

An area that JTF ARES can address pertains to increased U.S. freedom to maneuver in social media, where ISIL currently has the operational and strategic advantage. It is important that the U.S. Government and DoD are not paralyzed in trying to get our message out, and it is relatively easy to get a message out to show what their (ISIL) actions are like. There are plenty of defectors that can help us, but to date we have chosen not to. This is something that CYBERCOM and DoD leadership should look into.

## PLANES, TRAINS AND AUTOMOBILES (AND SHIPS)

*Mr. Joe Weiss, Applied Control Systems*
*Mr. Matthew Cockhorse, Battelle*
*Dr. Ray Better, Director for CRUSER (Robotics), Naval Postgraduate School*
*Mr. Mark Nelson, Director, Sierra Nevada Corporation*

During this panel, panel members and participants discussed robotics and unmanned systems, aircraft and SCADA systems, industrial control systems, automobile systems, hacking of automated and interconnected automobiles, challenges and opportunities of automated systems and vehicles, and second and third order effects of autonomy.

### Robotics and Unmanned Systems

The CRUSER program, a Secretary of the Navy sponsored consortium operated out of the NPS, is focused on robotics and unmanned systems education and research. During a recent NPS sponsored Hack-a-Thon (Hack the Skies) in San Francisco, NPS provided the code base used to fly its fifty autonomous vehicles in a decentralized swarm. There was no human control from take-off to landing, and while these vehicles were conducting combat search and rescue profiles, NPS invited the hacker community to help NPS identity flaws in its systems and how we can improve them, not just in our systems but also in general as the military has to engage with swarming systems both on our side and almost certain with our opponents. We also asked the hacker community on how we can best secure and protect them.

This event is co-hosted by the NPS Cyber Warfare Center and our Robotics Consortium. The reason NPS did this is in large part that all autonomous systems are in cyberspace – they have processors and that is where they exist. We cannot be talking about Robotics and Autonomous Systems and not deal with the cybersecurity aspects and efficiency that go with cyber systems as well. Within the DoD, we are running fast with planes, trains, automobiles, swarms, and jellyfish. On the latter, MIT and ONR developed robotic jellyfish that actually use ocean currents to move itself around. These jellyfish are also networks that can transfer information about what we are leaving on the seabed or in the water or moving through the battlespace. On land we can do similar things with swarms that use such things as insects (e.g., DARPA's hybrid robotic insect systems). For the CRUSER program, there are a lot of areas that are important in the cyber domain and we have to be smart about how to deal with them. With its focus on military operating systems, NPS recently went out and examined operating systems in the Navy, to include operator's use of cybersecurity practices for vehicles that could be exposed to the opponent. The good news was that they had passwords, the bad news was that it was oftentimes a single digit, and just to make sure they did not forget it, it was written down in instructions. NPS noted that operators contend that it is the cyber guys' job to figure out how to protect their cyber systems. That barrier and mindset is one that needs to be broken down. There are very few, if any, operators that do not operate without a cyber system, but security is something they set aside. How do we think about security in systems that are going to fall into enemy's hands while operating in enemy territory – in these instances we cannot afford to put high-end NSA encryption on everything we fly or drive or float while we are operating in harm's way. We have to find a better way to deal with those types of security risks. It may be an operational cyber risk management model that helps us scale well and provide good enough protection that operators can and will use, versus using high end protection where everything is a national secret. These are some of the interests we have in the intersection of robotics and cyber, as these autonomous systems will be used in enemy territory.

### Aircraft and SCADA Systems

Within the Sierra Nevada Corporation (SNC), aircraft is a big challenge when dealing with the cyber protection and security dimension. United Aircraft approached SNC and asked what kind of solutions SNC had to protect their aircraft and control systems (SCADA). SNC is not a boundary protection company, and continue to state that while many organizations such as United Aircraft think about firewalls when needing some form of boundary protection, they also have to assume that high tech adversaries have already learned had to get inside. The SNC approach is to assume the bad guys are already inside, and look at it from an inside-out perspective, and that this mindset needs to be assumed by others with vested in protecting and securing our systems and networks.

SNC has fielded SCADA protection systems that are already running with commercial power plants and fully tested. SNC's focus includes looking at the bad guys from the inside-out, and then setting up a way for these plants to manage the right commands from the inside. What the bad guys don't like is the fact that they cannot tell industrial control systems to do something that will cause damage or harm, e.g., they cannot tell the Hoover Dam to open its flood gates…it is not going to happen. Even if it is a false (lie) command or real command, the system will not accept and act on that command. SNC's goal is to have a set of rules and valid commands from the inside-out, and if adversaries are able to maneuver from the inside, there needs to be a reliable technique that can actually prevent adversaries from doing something bad from the inside out. SNC is testing those systems right now, and have built and delivered some of these systems.

When thinking about that SCADA-power plant side, we are working with the Naval Air Systems Command (NAVAIR). Any place where NAVAIR's aircraft have a control system at the front end of the plane touching something in the back end IT system, these are the areas SNC focuses on from the inside (middle). SNC not only does that on the SCADA side, they do it on the wireless side, such as its wireless penetration systems training focused on wireless techniques for defense and offensive operations.

**Industrial Control Systems**

Up until 2000, ACS focused on developing, operating and maintaining vulnerable control systems because they were reliable, efficient, and they did everything we wanted them to do. However, ACS noted that every one of these control systems went the exact opposite direction of security. It was nearly impossible to get people to integrate security into their systems, as this community works on the KISS principle. Cyber takes ICS in the exact opposite direction, and it almost by definition makes these systems less reliable. We have to figure how to get around that. The International Society of Automation (ISA) has developed international standards on control systems cybersecurity (ISA 99). DoD and the U.S. Government need to get more involved, as the equipment being used is the exact same equipment in every single DoD application – a controller is a controller and a sensor is a sensor. There is no difference in what the commercial world is using and what the DoD is using.

In the mid-1990's, the Kingston Steam Plant, an automated coal plant, automated all the rail engines as well as the coal delivery. Everything was automated, and done so with no thought of security.

When talking about swarms, one of the key things about wireless is that wireless is used in refineries and nuclear plants, and they are used in explosive situations. Securing wireless communication devices is important.

**Automobile Systems**

Battelle is a private R&D company who is the managing M&O for several of the DOE national laboratories. Battelle supports full spectrum cyber operations, both offensive and defensive, and seeks to strike that balance of understanding how to leverage attack techniques and understanding those techniques to better understand in order to defend systems and vice versa. From an automotive standpoint, Battelle has been working with the automotive industry on security for about five years, right when it stood up its cyber business unit. What was eye opening that in spite of the five years of R&D in this space to protect vehicles, one of the major OEMs in Detroit had more less interest (at the time) in talking to Battelle about protecting your vehicles with cybersecurity, and greater interest in talking about how Battelle could help them out with their workstations (response) as they did not have a security team. The automotive industry has really had to go through a period of rapid change these past several years, much of which has been reactionary. There have been positive movements, but there is still a long way to go. Battelle has done a lot of work on penetration tests on vehicles, and on developing bolt on security mechanisms to make sure if an attack does happen, it is not catastrophic to the vehicle system(s). Battelle also conducts its R&D with partners focused in developing highly verified specified communications systems that will make it mathematically impossible for ill-formed messages to make their way into the vehicle.

**Hacking of Automated and Interconnected Automobiles**

The death of the American actor of Russian origin, Anton Yelchin, because of the defective electronic gear shift lever of his vehicle, brought up conversation again about vehicle safety and raises the issue of an adversary potentially marketing various tools and techniques for vehicle hacks.

There have already been publicized vehicle attacks, which actually started five years ago when University of Washington researchers successfully demonstrated remote vehicle attacks. The terrifying thing was that most of those attacks that were publicized were still going unpatched. These vehicle manufacturers have not issued a recall for the most part to fix the problems in these vehicles. The other terrifying fact was that you had all of these unpatched vehicles on the road with known attack techniques that were developed for really low cost. An independent researcher had a $300 thousand DARPA Cyber Fast Track contract to do the first investigation. There are not a lot of costs associated with these attacks, but vehicles were also not randomly running off the road each day due to cyber-attacks either when these vulnerabilities were disclosed. From a nation state level, and an espionage and covert actions standpoint, they may overlap in the near future. There is no doubt that non-state actors will wind up in the mix in some dark place.

There is a lack of cyber forensics when you start talking about control systems, to include those in automobiles. In the IT world you have cyber forensics so you know (it may take a while) that you have been hacked. When you talk about industrial devices (and that includes planes, trains, automobiles, and ships), when these crash, the issue becomes how do you know it is due to a cyber attack? This is a problem, as if you don’t know what is cyber, how do you get attribution? Of the sixty nuclear control system incidents to date, none have been identified as cyber. Really? The issue when you have these automotive crashes is how do you distinguish between a problem and a cyber problem?

SNC has just started talking with the automotive industry. Part of our problem coming from the defense side is the automotive business model is different. The commercial business model is very different than a military business model – they are concerned with how do they build something they can use at a low enough volume that they can buy in bulk. Google is making these automatic cars, and no matter what you say there will be more and more in the future. These raise their own cybersecurity issues (from a wireless to a GPS or whatever control mechanisms they use) as every opening is susceptible to exploitation. Agree with cyber forensics in that you need to collect and analyze data elements to prove or disprove that something happened.

We should not be terrified unless someone wants to kill us and there are lots of ways for them to do it than hacking our automobiles.  What is more worrisome, and something to consider in our Smart Cities, is that there will be highly automated highway systems in our near future where we have decentralized control and all of our cars are talking to one another, and someone can bring all those cars to a stop. That kind of thing, where our highway systems affect our infrastructure systems in large scale, is indeed something to worry about those because that is a viable target for both state and non-state actors that have real resources.  As a member of the Defense establishment, we should worry about brass rings such as those things that are embedded into all automobile systems or gets across all your control systems for water or power – those kinds of things can be serious threats. Not everything is an attack, and we need not to over focus on the little things at the expense of the really big things that will make a difference on the battlefield and for society.  The nuisance threats we should leave to others to work.

While individualized attacks on vehicles should not keep us up at night, vehicle to vehicle communications are not required in order to have a large scale attack on automotive systems.  In the DARPA Cyber Fast Track project (vehicle attack demonstration), there were 471,000 vehicles were on the road that were publicly addressable at the time of the demonstration.  Researchers had a user interface they developed for very low cost that showed a significant number of vehicles on the road that they could just hit buttons and vehicles could have been disrupted or destroyed (C4 MAX+ telematics gateway unit). C4 MAX+ is used in a lot of busses and trucks, and they have a remote exploit that allows you to send command over to that unit.  Imagine what happens if a terrorist takes a bomb and blows up one bus, it causes terror (kinetic attack).  Driving hundreds and thousands of vehicles off the road with a cyber attack (non-kinetic attack) would have a more massive effect. All an adversary needs to do is instill terror and undermine the confidence in our ability in the transportation, and our ability to move from place to place and not have a dramatic effect.

However, the access required and the amount of planning and coordination required to pull off such a mass attacks against many different automobile systems with different software running would be monumental, but the psychological effect of targeted attacks against some busses running those controls would be massive enough, and it would be very low cost.

## Legalities, Liabilities and Benefits of Automated Systems and Vehicles

Google's "self-driven cars" and other future self-driving cars are designed to navigate safely through city streets. Many have sensors designed to detect objects as far as two football fields away in all directions, including pedestrians, cyclists and vehicles.  The car's software processes all the information to help the car safely navigate the road without getting tired or distracted.

It going to be interesting to see who is for self-driving cars, and who is against them.  A lot of issues from the legal side. DUIs would decrease with self-driving cars, but what happens when the car malfunctions? Who do you blame?  Who would be sued?  The technology is there, but if you are driving the newest Subaru, do you trust the vehicle to stop when it says it is going to stop?  Do you trust in its safety features to prevent accidents, even when it seeks to take human error out of the question for making adjustments to the various environmental and road conditions?

Four years ago, Navy leadership at Pentagon stated that our nation would not have anything approaching full autonomy, and that we need not to worry about that as that is decades away. This statement was obviously disproved, as technology to do these “automotive, self-driving” things in a benign environment is pretty much here. If you try to think about how autonomy compares to systems, it is going to be better on average, and it will save lives, but do we ever want to be in them on a large scale basis. With autonomous systems, we are talking about localized autonomy, and the car does not decide it wants to go somewhere. Instead, if you want to go somewhere, the car is able to operate under a set of controlled conditions.

There should be less worry about automated robots. It is easy for us to use robots as security guards, and much cheaper, and they are starting to show up on campuses, firms, and shopping malls. There was resistance at first, but they are increasingly being used. When talking about warfare with hypersonic and speed of light weapons, humans are just not going to make the decisions – autonomous systems are going to make the decisions. We are going to have to address the issues that are discussed there. The information age is the vestige of the industrial age. The problem of these systems is that we have relied on this mass produced, common chip recently such as those produced by Intel, and they are very versatile in that they can be placed almost anywhere. We can (and should) now go back to customized chips, as the economics can now support that. When we can get to the point if having multiple operating systems and customized chips from different producers, we make the attackers job a lot tougher. We should be looking for ways in our autonomous world to go back to specialized chips that only support a limited set of activities so it becomes very difficult for opponents, and economically, they are going to want to have to go after something. In the autonomous world, everything we do is going to be challenged by computational systems. Within Japan, more than 30 percent of their crop dusting is performed with autonomous systems – these systems look for insects on plants, then applies, and if clean, does not apply. Many of these systems have already taken over functions previously performed by humans (but that is a different discussion).

**Second and Third Order Effects of Autonomy**

In terms of what we will see in second and third order effects of autonomy, there will no doubt be liabilities and litigation for the private sector companies who are building autonomous systems. There is a net benefit for autonomy in the transportation sector such as saving lives, but liabilities are going to shift to a handful of companies that taking risks in taking these systems to market. There could be an issue when the first order cyber effect against a vehicle that kills someone, e.g., that first known that first known bug that kills someone in an autonomous vehicle. This will be really complicated in how we want to handle that as a society. The other thing to consider is that most breaches against major corporations have not caused a drop in their stock prices, because shareholders have gone numb to cyber attacks. This will be different when people start losing their lives because of current and future automated products that companies are putting out there, and there will be companies that disappear because of liabilities.

The DARPA High-Assurance Cyber Military Systems (HACMS) program offers potential solutions for an organization willing to conduct formal verification of software and hardware to ensure a more reliable and secure product offering. This program has been around for decades but has not been able to go mainstream. In using this approach, a military organization (or any other organization) could formally and mathematically specify all the code it is writing before they actually write the code, and then verify that it only does that functionality using a theorem prover or solver. This is important in that the focus was not invulnerability, but instead obtaining high-assurance cyber military systems…the 99% solution in 5-10% of the effort. This enabled us to take a helicopter and build a new operating system in a domain specific language that did not have the vulnerabilities seen in other software, and secure data bases using corollary verified protocols, and create a system that Red Teams did not defeat. Where we are with IoT and autonomous systems, the only real solution is to design security into systems from the very beginning, and to start leveraging these advances in formal verification and formal methods to design secure systems. It has not caught on yet, as cost was infeasible in context of profit margins. The rapid advance of current technologies within the research community continue to make this process potentially just as fast to develop something that is formally verified because you do not have to test it anymore. You are mathematically proving the functionality versus conducting a bunch of test cases which saves on labor (and saves scarce dollars in the process). If you can train people to do that correctly, and the market can take care of that if there are systems requiring this methodology, we can have very reliable, purpose built systems. IoT devices do not need to be a general purpose computer where it needs to run MS Word. They need to do a couple of things but do these reliably, especially when they are safety critical devices. This is where formal models and verification comes into play.

There is a real possibility of a financial collapse in the U.S. if an adversary can bring the electric grid down for a lengthy period of time, e.g., nine to eighteen months. This is not real hard for a determined adversary to accomplish. Organizations such as Moody's and insurance companies have to start to look at life differently, and they cannot miss what they missed before. In looking at formal methods, what we have not addressed is cyber and the cyber aspect. What we have done with formal methods is to look at things such as mean time between failure and other metrics, and not that someone would intentionally change the system which is really different. In looking at the Airbus crash in Spain, this resulted from a faulty fuel system, a control system, and they had not addressed some of the more esoteric issues that were system of system issues. We need to understand how formal methods will be applied when you start talking about the malicious and intentional change, because that is not how original formal methods were based on. What about Volkswagen? Normally we think about a rogue insider when you think about an insider, but in this case company leadership assumed the role of the rogue insider. What this truly malicious, as this was about (not the first) instantiation of an organization using cheat devices. EPA came up with a requirement that Volkswagen could not meet, but who was affected by this "malicious activity" is a different matter, and most likely just another lawyers or government institutions. What is happening is that cyber is driving issues. We live with redundancy and diversity in nuclear world, so what do you do when you put redundant systems on the same software or logic link? We have not looked closely into the logical separation (islanding) issue, we just looked at the physical separation, and we need to start rethinking what we are doing in the world of cyber, as it makes our life very different.

In Battelle fielded experimentation programs, there were a lot of small companies with new technology who came out and try to show where it might help the military. Battelle was funded by Operational Flight Program (OFP) to do it for the COCOMs. One of the things Battelle offered was a vulnerability assessment team, but to these small companies, they could not afford to worry about Cyber at all until they find out if they had a product that someone (in this case, the government) wants to buy. Any upfront cost for security before you find out that it is useful is not likely going to be supported by corporate leadership, and nobody going to build it in unless there is part of the contract that pays them to do it. Formal methods are not something generally applied to cyber warfare. Even when applied to simple tests, companies agreeing to this cyber examination took the information and changed their product, but stated they would not have spent a dime to go out and find out what they needed to do to change their product. This is a perfect example of an organization believing that the government is responsible for cybersecurity which is a challenges for those in the government sphere. The government needs to completely understand that there is a great economic engine out there in the rest of the country that has very different drivers and incentives, and that until something reaches a certain level of litigation, or it involves a lawsuit, or if it is a contractual requirement contract – smaller organizations do not have (or will not use) the resources to worry about cybersecurity until required to do so by the government.

As for litigation, it might not be as big a hurdle as we think. When something goes wrong with your car, there is a recall by the manufacturer of that vehicle. So if you look at installing computer software in a self-driving car, who provided that car with that software is the likely one to be responsible (what the car manufacturer initiates with the software developer is their problem).

If manufacturers are to build a car, and a computer to be able to control things, they need to include a switch that the operator can control. In this case, when car goes awry, there needs to be a way to immediately turn control to operator. There should always be mechanical back-ups. If we go the fully automated route, what is the back-up emergency control plan?

In industrial control systems, to include those going into automobiles, safety needs to be the key factor, and manufacturer must have a fall back to make sure nothing bad happens. We should not have safety devices anywhere connected to the Internet, in any way, shape, or form. Control is one thing but safety is something different. What is happening is that in the past we had separated control and safety loops, but we are now bringing these into the same device and same network. This is not a smart action, and is something we need to rethink before going too far down the path of automation in those systems, weapons and platforms with control systems as critical components (and when safety matters).

If there is not a sponsor or customer requirement, or some echo on what people want, you leave it corporations to use oftentimes scarce IR&D funds to develop our own solutions that work and of value to the sponsor, or that do not work and not of value. This process results in a lot of time and money wasted for these corporations, and products sitting on the shelves. The National Cyber Range (NCR) offering its range and/or some other certification authority that is free would be great and of potential significant interest to companies. Some small business technologists do not know how to test their systems from a cybersecurity perspective, and many do not even have a test plan that results in them not even being able to test their own devices correctly. The government (and possibly academia or larger companies with cyber expertise) might need to mentor these guys.

# Day Three – June 23, 2016

## The Internet of Everything and the Impact on National Security – Considerations for Operating in Cyber Cities

### MORNING SESSIONS (AM)

**Future Urban Operations**
*SGM Richard Russo, Joint Interagency Task Force*
*MAJ Derek Smith, J5 Transregional Threats Coordination Cell*
*Mr. Justin Valdego, Carnegie Mellon University*

**Intelligence Preparation of the Cyber Domain**
*Mr. Ronald Carback, DIA*
*CDR Pablo Breur, NPS*
*CAPT Daniel Verheul, Center for Innovation and Innovation*
*CDR Christopher Hoffman, Office of Naval Intelligence*

**Project Blackbeard and Beyond**
*LT Tyson Meadors, NPS*

### AFTERNOON SESSIONS (PM)

**OCONUS Threats and Challenges**
*Lt Col Lauren Courchaine, EUCOM Joint Cyber Center*
*Dr. Fuzzy Wells, PACOM Cyber War Innovation Center*
*Capt Brandon Johns, DIUx*
*MG(Ret) John Davis, USA, Palo Alto Networks*

**Cyber Capabilities and Limitations**
*Mr. TR Koncher, Lawrence Livermore National Laboratory*
*Dr. Matt Leahy, MIT Lincoln Laboratory*
*LCDR Thomas Parker, Navy Cyber Warfare Development Group*

**DoD Way Forward**
*Dr. Hy Rothstein, DoD IOCR at NPS*
*MG(Ret) John Davos, USA, Palo Alto Networks*
*COL James Chatfield, DCS G-3/5/7 Operations Plans & Training, 335th SC(T)*
*Capt Brandon Johns, DIUx*

## Considerations for Operating in Cyber Cities

The third day of Cyber Endeavour 2016 was conducted at the classified level. The following threads and topics were discussed:

- Future Urban Operations
- Intelligence Preparation of the Cyber Domain
- Project Blackbeard
- OCONUS Threads and Challenges
- Cyber Capabilities and Limitations
- Department of Defense Way Forward

## Key (Unclassified) Takeaways

The following are key unclassified takeaways from Day Three panel discussions and special guest presentations:

- We need more trust-based leadership. The reason we can't/don't have more creative innovation is because we don't trust. We are risk adverse.
- No one operates in a cyber-free environment. Even in countries where only 30 percent of the population have access to electrical power, close to 100 percent have cell phone usage.
- Quit telling cyber experts to "do something;" just like anyone else, give them a mission and let them work it out.
- Our military institutions demand career breadth, which isn't necessary attractive to cyber experts who prefer to focus narrowly on their field of expertise.
- Everyone wants to do offense, but don't forget defense: You don't need permission to do defense.
- We have a lot of smart partners. We don't need to replicate capabilities that we can share with our partners.

- We’ll never have enough people to get out of ‘this;’ automate more and reduce dependence upon people and human error.

**Follow-Up Classified Discussions and Information Requests**

Cyber Endeavour 2016 participants who attended the third day of the conference, and who still have the appropriate TS/SCI clearance, are encouraged to contact the DoD IOCR directly to discuss and/or review any classified materials, documents, and associated notes from day three panels and special guest presentations.