Nov 8th 2015

Executive Summary (First Report)

This document is draft and issued by Cyber^3 Conference Okinawa 2015

Track A Summary: Cyber Connection

3 Main Issues:

1. **Education:**

There is a vital need to educate industry stakeholders, governments and consumers about the IoT – both opportunities and risks. Currently, there is a widespread lack of public trust regarding new technology paradigms. We must accept (and explain) that there is an unavoidable risk-benefit balance: As benefits increase, so goes risk.

AI and automation technologies can make the public's lives safer and more comfortable – but companies must earn trust and foster understanding. By 2020, 15-20 billion devices will be connected to the Internet through a seamless cloud. No one, not even technologists, fully grasps the enormity of that coming reality. How do we educate the public in a meaningful way? Humans interface with technology without thinking about it and the amount and nature of personal data is constantly changing, so even education aims at a moving target. As consumers become able to clearly identify and understand benefits, acceptance of new technologies inevitably increases (e.g. Web mail — no one thought it was safe when it was introduced, now no one can live without it). The same trend will continue with IoT and this will generate a new wave of digital data about users.

2. **Creating Structure:**

For this reason, it is essential to determine an architecture for the IOT. The biggest point, from a security standpoint, is to develop **resilience** in order to prepare for unknown threats. Nik calls this "thinking the unthinkable". It means assuming that some threats are unstoppable, so rather than trying to defend against every unknown, we need systems that sustain compromise and keep on functioning with minimal inconvenience.

In the future, network users will no longer be only humans – robots and AI systems are becoming part of the cyber universe. The Internet must be equipped to smoothly manage interfacing with IoT devices, not just the other way around. Autonymous systems can be attacked and compromised, so they must have defense mechanisms that can operate—at least at some level—without human intervention.

The IoT, by definition, implies a massive increase in data being collected and transmitted. With that increase in the volume of data there is a concomitant increase in vulnerabilities. Hence, the IoT will usher in a new era of multifaceted vulnerabilities. How can multi-stakeholder dialogue create processes that will foster genuine cooperation, deal with national regulatory regimes encumbered by problematic relationships, and ultimately, deepen public trust? It is essential to establish a shared-goal-driven multi-stakeholder network to develop regulations and security standards for IoT; we need to find a workable balance between unfettered access and extremely limited innovation. This can only be achieved through the active cooperation of a body of diverse stakeholders.

Furthermore, the IoT can maximize & optimize device functionality, benefitting humans by providing contextual experience and enabling mass customization. At the same time, we have to address the necessity of building security into every element of these future networks. The "hyper-connected" world also means that closed/protected innovation will give way to open innovation. Data is becoming the coin of kingdom in the age of IoT. More data is being produced than ever before; analyzing and leveraging this data is a key future challenge.

For industrial IoT security, the security of a whole chain must be ensured by a group of diverse stakeholders. Resilience is key to preparing a secure IoT future; anything that can be hacked, will be hacked. Even non-networked (e.g. voting machines) systems are at risk. Back-up systems must be in place to mitigate this. Barrier-based (purely defensive) protection is already becoming obsolete. The best model is something like the body's immune system: a complex system that

sustains myriad attacks daily, but manages these attacks through flexible responses so as to preserve functionality with minimal impact at the day to day level. The system may function for years without succumbing to any serious effects of malware intrusions.

3. **Human Factors and the Moral Dimension:**
There are undeniably serious questions of privacy, human rights, and legal/moral responsibility with regard to the IoT and AI. We must consider what is the best approach to regulating the IoT. On the one hand, a non-regulated world would be a frightening, unusable "jungle," but on the other hand, we could easily create an over-regulated "nanny state". Liability must be clearly established in the event of an attack or accident involving autonomous devices. In order to make AI effective, we must study human decision-making and interaction and apply these insights to our technology. Ultimately, the solutions to current and future issues are not just technical, but social, political, and economic.
IoT could provide increased access and freedom to users in emerging markets, but in emerging economies technology tends to be more expensive than human resources, and IT governance is more lax. We must ensure that knowledge creation does not merely replicate the current state of economic and social inequality, but will bring tangible benefits to all, not just those who can afford them. IoT must not cause damage when implemented in user-based applications (home, office etc.). The digital Hippocratic Oath of IoT should be, "First, do no harm."

Track B Summary: Cyber Security

3 Main Issues:

1. Cyber Security as the Fifth Domain of War:

Traditional precepts of war such as proportionality and mutual assured destruction break down when applied to nation state activities within the Cyber realm. While Cyber attacks could conceivably cause the same degree of massive destruction as a nuclear or biochemical attack, that is not necessarily the case. A Cyber attack can have a much narrower focus than a nuclear or chemical attack, and this helps explain why nation states have been willing to engage in offensive Cyber activities and even nations who have withdrawn from conventional warfare and who have refrained from using tactical nuclear or other weapons of mass destruction are willing to consider Cyber warfare. The shared use of Internet infrastructure by military and civilian users makes it difficult to distinguish military targets from civilian collateral. This problem is compounded by uncertainty over the secondary and tertiary impacts of an attack. Moreover, the technical difficulties in conclusively identifying the source of an online attack make traditional risk calculations difficult to apply when evaluating options to deal with a Cyber adversary.

Many nation states are actively engaged in Cyber espionage as well as limited amounts of more offensive activities. Establishing common "rules of the road" (along the lines of the "Gentleman's game of espionage" during the Cold War) is an essential step if nations are to avoid an accidental escalation of Cyber activities into a full-fledged Cyber war. The relative ease with which a Cyber weapon can be developed or deployed by a non-state actor further increases the need for nation states to establish common understandings, whether formal or informal, as to what kind of behavior is acceptable.

Viewed in the most general sense, the idea of nations-in-conflict working out an overarching agreement as to what types of Cyber activities are permissible and what types are not seems unlikely. However, when the problem is broken down into discrete issues, specific areas of common concern and common values can be tackled first. Over time, we believe that it is possible to make progress toward establishing a multilateral dialog on nation-state Cyber activity that will contribute to stability and security for all parties and, equally important, their citizens.

International law makes no distinction between Cyber war and other forms of war, so this body of law can be brought to bear. Attribution is a crucial element of any response, so more effort should be put into developing capabilities that will assist nations in identifying the origin of attacks. There are 3 critical areas where nations can enhance their attribution capabilities: better technology, better thread data sharing, and shared intelligence assessments of adversaries. Without this, nations will not be able to differentiate between activities by other nations and those by non-state

actors, nor will they be able to respond appropriately to either. In fact, identifying threats from non-state actors might be one area where traditionally hostile superpowers could find a level of common interest, and that could facilitate the process of establishing rules. Moving forward, these nations should identify mutually agreed-upon sensitive areas — nuclear plants, financial systems, etc. — that all parties will agree are off limits. Agreements not to violate each other's most sensitive infrastructure are only part of a bigger picture that needs more development. President Obama has already discussed common concerns with Premier Xi, President Park, and Prime Minister Abe.

Cyber defense is really the first concern of nation states in the Cyber realm. Threat data sharing mechanisms (both government to government and private sector to public sector) can contribute to a nation's ability to fend off attacks. To be useful, however, these mechanisms must allow for the collection of meaningful data that groups can act on. Otherwise, the data sharing becomes just another report that nobody reads. While retaliation should remain a tool of sovereign powers only, there is also room for the private sector to assist in responding to attacks thru tool development and network management.

There are other steps that must be taken as well. Building resilient systems that move the most sensitive or volatile elements behind multi-tiered defenses is required. Firms that are hacked have a right to self-defense, but it is unclear whether that right extends to hacking back, particularly when that involves destroying or disabling the hacker's assets. While there have been maritime privateers in the past who had permission to hunt down and destroy an adversary's ships, it is not clear that such behavior is possible, much less desirable today in the Cyber realm.

The issue of economic espionage is particularly difficult because it requires nation states to reach agreements in an area where normative values are not shared among superpowers. Indeed, the scope of economic espionage itself can be called into question. For example, the use of economic espionage by nations engaged in trade negotiations is beneficial to companies based in a nation that has privileged access and insight into a rival's negotiating position. These difficult issues can only be solved, however, if countries are willing to engage each other in bilateral and multilateral forums and begin the process of finding common ground.

2. Olympic Security:

The London Olympic security team dealt with five distinct networks, each of which required its own security architecture:

- the LOCOG operator's corporate LAN
- the scoring network that transmitted scores and game data
- the press network
- the broadcast network
- a public access WIFI network

The network operators installed the usual firewalls, IDS, and anti-virus defenses, but in addition, they created a big data analytical machine that sampled traffic and looked for less obvious signs of ongoing intrusions. The number of attacks registered — 11,000 per second — required a huge amount of processing power. More importantly, it required planning, practice, and a firm grasp of the full nature of the risks faced – by the Olympic village, by its sponsors, the visiting dignitaries, and the nation as a whole. The London Olympic security team engaged in a massive planning effort, which included prioritizing what needed protection. It also required a deep look at governance and an understanding of the roles and responsibilities of the various local actors — venue security, network security, police, etc. It also meant identifying the populations of visitors, contractors, press, and others that use Olympic network assets and the problems and risks that they bring. For example, logs showed malware activity emanating from devices brought onsite not only by visitors, but by press as well. Understanding these risks and dealing with them by such things as network segmentation is critical.

LOCOG and the UK Government initiated a number of new efforts that facilitated their ability to respond rapidly and effectively to emerging threats. They established solid partnerships with the security services of nations expected to participate in the Olympics, not only leveraging best

practices across the collective brain trust and expanding capabilities beyond the norms of UK security and police forces, but also creating a sense of common cause amongst the coalition participating in the Olympics. These relationships paid huge dividends during the Games where intelligence feeds, real-time analysis, and course-of-action formulation were supported broadly across the Olympic coalition. The host government should provide an onsite fusion center where other governments and stakeholders can set up operations and share threat data as problems develop. LOCOG also engaged in a series of technology freezes with the goal of minimizing the threat of new vulnerabilities being introduced by new technology. Unfortunately, this principle must give way to the technological needs of users. In London's case, the explosion in WiFi devices led to a late decision to add a public access WIFI network. Governance must be worked out. The roles and responsibilities of security teams—everyone from the police to private security—must be understood and personal relationships must be established so that groups know who to turn to for help. Once the initial planning is done, security staff must be trained and drilled extensively. Red teaming and scenarios must be used to test and refine responses. Physical and Cyber security must coordinate. Physical access enables access to IT assets and IT assets enable physical access. Adversaries understand this. Security teams must be able to coordinate across multiple attack vectors—from physical ingress/egress points to authentication fraud to DDOS, etc. This is what teaches them the kinds of real problems they will face and puts them in touch with the counterparts with whom they must work to resolve incidents. Unlike the military, the Olympic committee does not control all of the security assets involved, but outside groups, whether police or foreign security teams, share a unity of purpose. Establishing trusting, personal relationships can substitute for a chain of command and ensure that teams coordinate on developing issues quickly. Rio de Janeiro used the recent World Cup games to train its security teams for the upcoming 2016 Olympics. Tokyo should make sure the security assets deployed for the 2019 World Rugby Cup are the same assets that will be deployed in 2020.

The next Olympics will surely face almost every sort of threat imaginable. It is therefore crucial to assess and plan for a wide array of threats — hacktivists, organized crime, insiders, state-sponsored hackers, and terrorists. Each adversary's psyche must be profiled and, to the extent possible, potential attack vectors must be identified and neutralized. As we saw with the Germanwings' co-pilot who intentionally crashed a commercial airliner earlier this year, safeguards (in this case, locks on cabin doors) designed to thwart last year's attack can open up new and deadly attack vectors. We still need to make best-guess predictions about what an adversary will do and then take appropriate countermeasures, but we must not become complacent: we must assume that new and unexpected attack vectors will appear, and we must plan as best we can to deal with those events as they happen or as they are discovered. The Olympic Games raise a nation's profile and security teams must be prepared for attacks against a variety of targets—the energy grid, sponsors, government sites—and not just the Olympic website and village network.

An interesting example of getting one step ahead of an adversary's thinking was the real-world problem of how to deal with hooligans at the last European football championship. The event sponsors cleverly invited police from various EU nations that had a history of hooligan violence at games to appear at the championships wearing their local uniforms. Surprisingly, the plan worked. Hooligans were much more reluctant to misbehave when police from their home countries were visible. It would be worth considering the benefits of allowing Japanese police and police from neighboring countries to share threat data in real time. By planning, practicing, and working together, Japan and Korea's event managers can minimize the threat to their events, and ensure that the upcoming Olympics are enjoyable for all.

3. Cyber Regulation:

Cyber Regulation is the middleware that ties big picture concepts such as nation state security goals to the tactical day-to-day issues such as managing a large-scale sporting event. Japan is positioned to be a showcase for Cyber regulation as a positive contributor to safety for the Internet. Japan is committed to Internet access for its citizens, but wants to ensure that this access is safe and contributes to the welfare of society. The key to successfully navigating the Internet, in the eyes of many EU counterparts, is to establish regulatory guidelines that embody the normative values and priorities of the member states. This includes building resilience, employing cross-border collaboration mechanisms, protecting infrastructure, and managing risk. At the same time,

citizen privacy and convenience must be respected. For this reason, issues such as net neutrality and data breach notification must be addressed as well. The goal is to strike the best balance between competing needs and interests in accord with established values and legal processes.

While the United States and EU scramble to address the recent High Court decision to nullify the Safe Harbor provisions used by US companies for storing EU citizen data, the EU must define its own internal rules in a way that fosters and does not inhibit innovation. While there remains a vital role for government, private sector firms must be actively involved as well. In a variety of ways, from initial threat response to new security tool developments, governments must rely on the private sector to lead the way. Privacy is a paramount concern, but it cannot be the only concern. Access to threat data and the ability to share data between government and private parties must be enshrined as well.

There is a tendency for media to seize on worst case scenarios in dealing with Cyber news, which contributes to misunderstanding and hysteria. Cyber regulation designed only to deal with worst case scenarios will be off the mark. Regulatory action must reflect a more measured, reasonable assessment of threats. In cases where certain threats are known, it is possible for government bodies to require that steps be taken to prevent or mitigate these known threats. Addressing APTs and zero-day threats is more difficult, but this fact alone does not justify a failure to act where threats are known and countermeasures are available.

The situation is analogous to the laws of the roads. Every nation has its own rules, but there are many commonalities. Complete harmonization is not required in order for countries to issue and honor international drivers licenses. The international driver must modify some driving practices to abide by the laws of a particular nation, but the process works, allowing countries to manage road safety in accord with local norms and international travelers to take advantage of the roadways in many countries. A similar approach should be considered for the legal and regulatory framework for Cyber, particularly as it pertains to the private sector. Each nation is free to implement its own rules, but there are certain core concepts (defense in depth) and factual realities (known threat vectors) that will ultimately play out (with variations) just about everywhere.

Businesses, particularly multinationals, are well positioned to assist nations in seeking out common strategies and standards. Much as the World Health Organization sets safety standards for the handling of epidemics and other health crises, a multi-stakeholder international organization could recommend best practices and minimum standards that would help nations in setting domestic rules while providing business with some level of consistency across markets. Otherwise, if nothing is done, the industry will develop unimpeded and possibly in ways that make later attempts to regulate it less effective. At the end of the day, each nation or multi-national body must establish rules that represent its values and its priorities, but collaborating to find common solutions and mechanisms for collaboration will serve the interests of all.

Track C Summary: Cybercrime

4 Main Issues:

1. The need for international frameworks to address cybercrime:

The Budapest Convention is a solid international framework for cooperation on cybercrime. The MLAT process, however, is not sufficiently agile or responsive. While much can and should be done to improve the existing processes, there is also a need to evolve approaches. Increased awareness is required to drive development of new approaches; however, those that emerge will likely be different and culturally conditioned. Socially accepted approaches will only emerge through early adoption of multi-stakeholder dialogue. As national security and law enforcement become more intertwined, we will see an inevitable increase in complexity.

2. Challenges in aligning policy & legal frameworks with the pace of technological innovation:

Public-private partnerships and flexible-outcomes goals (specifying desired goals without specifying how to achieve those goals) are favored because governments struggle with the pace of innovation. With increased nation state activity in cyberspace, new challenges emerge; it becomes difficult to ensure consequences for bad actors – either through prosecution or normative

frameworks – due to complexities of attribution (technical and political). Cyber risk must be integrated into enterprise risk management, making it a C-suite responsibility (not merely an IT responsibility) and both sides need to promote enterprise and government coordination on risk management.

3. Building coordinated public-private partnerships and information sharing to manage cyber risk:

Information sharing is an important tool, not an outcome and certainly not a panacea. It should not be solely focused on industry-to-government, but also industry-to-industry, government-to-industry, and government-to-government collaboration. There has been substantive progress made in information sharing and workable models for sharing. We need to learn from this (e.g. Interpol, Europol, Microsoft Cybercrime Center) and build on it. The "5 eyes" model is outdated, and collaboration should be looked at more through the lens of international multi-stakeholder cooperation. There will never be a global one-size-fits-all model, so we must accept diversity. Governments should be a participants, not gate-keepers in these efforts.

4. Emerging security and privacy challenges:

Future innovations will create both security and privacy challenges and new ways to address them. It is critical to learn and scale practices (e.g. security by design, authentication) that have been learned through the IT and operational technology (OT) waves, and transfer this knowledge to the IoT. We must continue to develop a skilled anti-cybercrime workforce for government (e.g. specialists in investigation and prosecution) and industry (security architects). We must recognize that there is no "leader" in information sharing (or in cyber security, for that matter). Everyone has made mistakes. We need to develop a best-practice model based on successes from around the globe.