INL/CON-16-39323
PREPRINT

Cyber Norms for Civilian Nuclear Power Plants

CyCon US (2016)

Christopher Spirito

October 2016

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Cyber Norms for Civilian Nuclear Power Plants

Christopher Spirito

Idaho National Laboratory
christopher.spirito@inl.gov

Abstract

The international community agrees that the safe operation of civilian nuclear infrastructure is in every population's best interest. One challenge each government must address is defining and agreeing to a set of acceptable norms of behavior in cyberspace as they relate to these facilities. The introduction of digital systems and networking technologies into these environments has led to the possibility that control and supporting computer systems are now accessible and exploitable, especially where interconnections to global information and communications technology (ICT) networks exist. The need for norms of behavior in cyberspace includes what is expected of system architects and cyber defenders as well as adversaries who should abide by rules of engagement even while conducting acts that violate national and international laws.

The goal of this paper is to offer three behavioral cyber norms to improve the overall security of the ICT and Operational Technology (OT) networks and systems that underlie the operations of nuclear facilities. These norms of behavior will be specifically defined with the goals of reducing the threats associated to the theft of nuclear materials, accidental release of radiation and sabotage of nuclear processes. These norms would also include instances where an unwitting attacker or intelligence collection entity inadvertently makes their way into a nuclear facility network or system and can recognize they are in a protected zone and an approach to ensuring that these zones are not exploitable by bad actors to place their sensitive cyber effect delivery systems.

I. Introduction

In 2015 the UN Group of Governmental Experts (GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security, adopted a consensus report[1] proposing norms of responsible behavior in cyberspace and how international law applies. The proposed GGE cyber norms include five limiting norms and six good practice and positive duty norms. (See Table 1 on Page 2) They are a necessary first step to establish both what behaviors like-minded nation-states will adhere to while operating within cyberspace and what types of responses cyber defenders can expect from their national cyber resources. This middle-ground we are operating within is a bit amorphous though as the proposed norms relating to critical infrastructure are both reasonable and absurd.

[1] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." August 31, 2015. Accessed July 11, 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

In a sense, any initial set of behavioral norms agreed to by cyber-capable nations such as the United States, Russia, China, Germany, France and Korea must be aspirational, where each country provides a generically good end-state that assumes political, economic and military concerns are somewhat satisfied. The GGE proposed norms that nation-states *should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure and should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/ CSIRTS),* are good examples of this contrast between what is reasonable and absurd. These behaviors, observed in a vacuum make sense and attempt to apply International Humanitarian Law to objects and capabilities in cyberspace such as treating national CERTs as the cyber equivalent to the Red Cross. Outside the vacuum there are at least three core problems at hand. First, adherence to these proposed norms requires nation states to be capable of observing the agreed upon behavior for norms compliance. This is of course a non-trivial problem in the cyber domain. Second, the vagueness of the norm does not adequately map to the range of possible actions in cyberspace. If nations do not explicitly describe which actions in cyberspace are allowable, such as reconnaissance or implantation activities, a perceivably non-aggressive activity performed against a mutually agreed upon critical infrastructure system could be viewed as a norm violation by the target nation. Third, military action planning often includes disabling key critical infrastructure systems, such as power grids, and these capabilities will not be removed from the option list until there is a commensurate effect that can be delivered.

Limiting norms:

1. states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
2. states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure;
3. states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions;
4. states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity;
5. states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age.2

Good practices and positive duties:

1. states should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices;
2. states should consider all relevant information in case of ICT incidents;
3. states should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs;
4. states should take appropriate measures to protect their critical infrastructure;
5. states should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts;
6. states should encourage responsible reporting of ICT vulnerabilities and should share remedies to these.

Table 1 : GGE Proposed Cyber Norms

The challenge faced by civilian nuclear power plants (NPPs) is in understanding how to use nation-state adopted norms to establish a set of cyber norms specific to their day-to-day operation. While it would be nice to assume that civilian NPPs, and CERTs for that matter, are not included on cyber-target lists, the reality is of course that they are and thus need an adequate protection and response plan for cyber actions commensurate with the physical security mechanisms already established. Using the GGE proposed norms this paper will offer up three cyber norms for civilian NPPs and a description of how they could be implemented.

II. Proposed Cyber Norms for Civilian Nuclear Power Plants

Over the past five years Idaho National Laboratory (INL) has provided support to the Office of Nuclear Security Cyber Security Program at the International Atomic Energy Agency (IAEA). The purpose of this program is to provide IAEA *member states with guidance and technical expertise to support the detection of, and response to, criminal or intentional cyber attacks involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities.*[2] The IAEA program includes consultancies throughout the year attended by member state representatives allowing for input and discussion on the challenges faced and the unique member state constraints of each of our national support infrastructures. These proposed cyber norms for civilian NPPs are intended to address observed gaps and promote healthy multinational behavior to ensure the safety of NPP operation and security of nuclear and radioactive material and information. They are in addition to many of the GGE proposed norms which would be considered cybersecurity best practices such as securing the supply chain, implementing existing best practices to raise the bar as high as possible for attackers, and including plant-wide cyber awareness training on a periodic basis such that all personnel are knowledgable of the actions they should be taking on a daily basis to reduce the attack surface and are aware of the internal processes and programs they should engage as needed.

Our three proposed cyber norms are:

1. **Consider the possibilities:** Nuclear Power Plant personnel should thoughtfully consider whether observed events within the business and control system networks may be the result of a cyber campaign or attack.
2. **Practice makes perfect:** Nuclear Power Plant incident response personnel should be routinely exchanging information within their vetted community of practitioners and exercising their cyber incident response communication plan with regional and/or national authorities.
3. **Active cyber defense:** Nuclear Power Plant cyber defenders should consider implementing non-traditional capabilities to shift attack identification earlier in the cyber attack lifecycle and improve their ability to actively engage with adversaries. This would include the use of available intelligence feeds and denial and deception activities.

The common theme that exists across these three proposed cyber norms is also the most uncomfortable aspect of these norms, namely that failure is encouraged. This is of course contrary to what the nuclear safety culture calls for and will likely be the most significant roadblock NPPs will face when implementing any of these norms. This is one of the drivers underlying the discussions within the international nuclear-cyber community on integrating security into the nuclear safety culture. While these norms could equally be considered as recommendations for improving the overall cyber-security posture and readiness of NPPs, if taken as recommendations and not expected norms of behavior, the desired outcomes will likely fall short. It is only when an organization fundamentally changes their behavior to be part of their daily business and operational processes that improved outcomes will be sustained long term.

---

[2] Dudenhoeffer, Don. "Office of Nuclear Security Cyber Security Program Overview." May 21, 2013. Accessed July 11, 2016. https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-21-05-24-TM-NPTD/day-1/5.cybersecurity-dudenhoeffer.pdf

III. Consider the possibilities

There are a few contributing factors to why NPP personnel have not considered a cyber attack as a root cause for observed events within their business and control system networks. The first factor is a general lack of awareness by nuclear operators of what different types of cyber attacks look like. In order to identify a cyber attack or at least be open to the possibility it is necessary for all personnel to be educated on the cyber attack lifecycle and the range of attacks that could and have occurred against NPPs in the past. The usual operating protocol in the event a system or device fails is to replace the device and its configuration such that the system is restored to the design basis. While this approach will meet the operational requirements for keeping nuclear power systems engaged, the process is often one where any forensic artifacts will not be preserved thus limiting an investigation into the cause of the component or system failure. A second contributing factor to not considering cyber as a root-cause is a lack of approachable processes or available tools for assessing both business and control systems that are experiencing issues. It is believed by the technical community that one of the underlying reasons for a lack of reporting of cyber events within nuclear facilities isn't because they are not occurring but because they are not recognized by nuclear plant operators.

INL recognizes that this norm is not an easy one to adopt as it requires NPP personnel to both alter their root-cause analytical processes and extend their discovery time per incident which in turn will eventually require additional resources. The INL believes that NPPs that recognize the importance of root cause analysis in conjunction with a reasonably good knowledge of the cyber domain will be more likely to proactively discover attacks in process and those that have already succeeded in penetrating their environment. The mid to long term benefit is that cyber-knowledgeable nuclear operators and engineers will be more likely to recognize a nation-state cyber campaign manifesting itself across business and control systems within the NPP environment. This change in behavior will also drive the adoption of the second norm we proposed: *Practice makes perfect.*

IV. Practice makes perfect

Information exchange norms are among the most common within the cyber domain including the GGE recommended norm on nation-states considering how best to cooperate to exchange information and assist each other in the prosecution of terrorists and criminals. Our extension of this norm has two important aspects to it related to our first proposed norm of c*onsidering the possibilities.* First, when operating within a new environment, such as the intersection of the nuclear and cyber domains, each incident or event will be an opportunity to apply investigative methods and tools to interesting (suspicious) events. The difficulty of course is that without a library of similar types of events to compare against, analysts are forced to make conclusions that may not be well informed. Analysts and incident response personnel are often limited by their operational environment and the knowledge-network connections (community of analysts) they have access to. The process by which an incident is analyzed and the results structured and shared should become part of each NPP operator and/or cyber defenders daily interactions with an emphasis on engaging broader knowledge-networks as events are validated, triaged or discarded. The second important aspect to this norm is operationalizing the incident response communication plan such that the channels are exercised on (ideally) a daily basis. The ability for an NPP to communicate to their national resources the current set of incidents/events will help to bridge the communication gap that often exists during moments of crisis. Engagement of these channels will allow terminology gaps to be shortened

ensuring that as incidents are reported from the NPP to national CERTs (if available) and competent authorities, that the appropriate context is understood preventing signaling and communication issues.

The value in information exchange comes not solely from the knowledge being shared but from the connections made between members of similar communities. Having a trusted network of experts will not only accelerate the incident analysis process through access to a larger library of events but will also provide each organization a shared-leadership role within the community as their own expertise is shared to the benefit of other analysts and their NPPs. Similar to what happened in the ICT space, as the number of closed incidents in the analysis queue increases, so do the list of observations on precursor events that may have indicated an attack was about to launch against the environment. The cyber security community loosely classify these events as left-of-hack as they exist before an incident is observed (or the attacker has made their way into your environment) and are a basis for our third proposed norm of *Active Defense*.

V. Active cyber defense

Active cyber defense (ACD), a term that describes a range of proactive actions that engage the adversary before and during a cyber incident, can dramatically improve efforts to prevent, detect and respond to these sophisticated attacks.[3] The cyber attack lifecycle defines six phases of activity, three before an attacker has penetrated your environment (reconnaissance, weaponization and delivery) and three after (control, execution and maintenance). Traditional information assurance and cyber defense models place most of the emphasis on proactive threat mitigation through best practice implementation and identification of known adversarial tactics and techniques, well described in the MITRE ATT&CK[4] model and framework. This approach while reasonable is also a bit like playing whack-a-mole where your incident handling team is reacting to anomalies without the ability to disrupt attacks before they occur. Our third proposed norm is for NPP operators and cyber defense personnel to implement what would be considered non-traditional or emerging capabilities to shift attack identification earlier in the cyber attack lifecycle.

The use of available intelligence feeds from both national resources such as law enforcement or intelligence agencies as well as private threat intelligence providers is a reasonable first step. Another capability that would be useful for NPPs to focus on is the use of denial and deception within their environment which will provide once a sufficient maturity level has been reached, a set of left-of-hack indicators of potential cyber attacks. Denial and deception methods include the management of deception objects (facts and fictions) and deception methods (mislead and ambiguity) such that an adversary is detected during the reconnaissance, weaponization and delivery phases of the cyber attack lifecycle.[5]

An example implementation is shown in Figure 1. In this example, an organization creates a set of false personas with web footprints similar to Robin Sage, the fictional cyber threat analyst created as part of a

---

[3] Lachow, Irv. "Active Cyber Defense - A Framework for Policymakers." Feb. 2013. http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf

[4] "Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)." Oct. 6, 2015. Accessed July 11, 2016. https://attack.mitre.org/wiki/Main_Page

[5] Heckman, K.E., Stech, F.J., Thomas, R.K., Schmoker, B., Tsow, A.W. *Cyber Denial, Deception and Counter Deception - A Framework for Supporting Active Cyber Defense.* Springer, 2015.

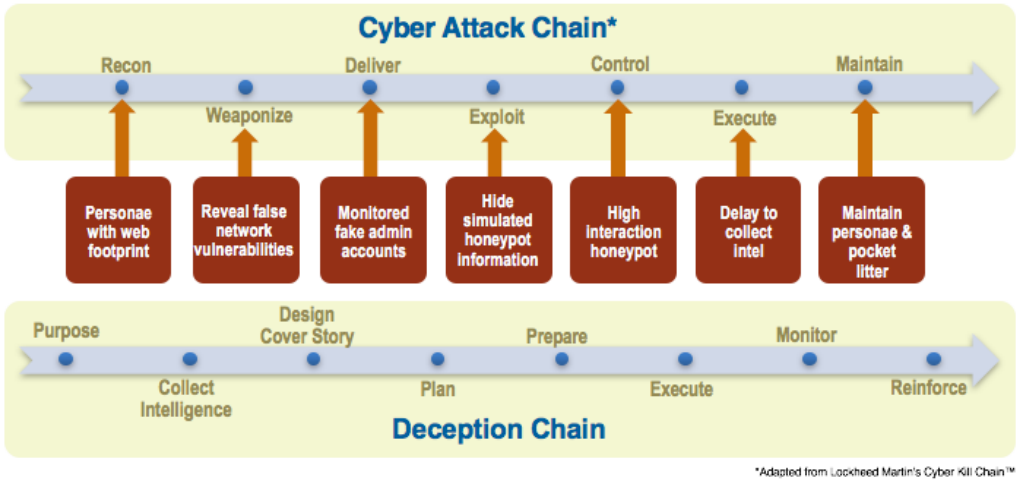

Figure 1 : Cyber Attack and Deception Chain

28-day experiment to test trust connections on social media primarily between active military and intelligence personnel and supporting contractors. This will aid in the discovery of reconnaissance activities that if observed are a reliable indicator of a future cyber attack. Revealing a set of false network vulnerabilities will help the adversary shape their attack and choose an appropriate implant package for the target environment. The false persona accounts will be monitored for all activity, but what we are specifically interested in are attempts to deliver weaponized payloads. Using these payloads, an organization would self-infect a controlled simulated environment, commonly known as a honeypot or honeynet, that would allow for their action to be observed as they attempt to fulfill their attack goals. This type of approach once refined would help to delay the collection of intelligence and prevent the exploitation of critical systems while building a set of threat actor observables that should then be shared with other community defenders. Dewan Chowdhury, the founder of MalCrawler, implemented part of this approach in 2015 and presented his findings at the 4CICS conference[6] where he described the varying behaviors of the actors they engaged. "Most of the activity was espionage: stealing technical data, mapping SCADA networks and installing additional malware. The groups had access to the Human-Machine-Interface (HMI) that would have allowed them to manipulate the grid, but Chinese, United States and Russian groups must have some informal agreement to leave grid functions alone. Middle Eastern actors tried to perform control actions to sabotage the grid."[7]

Following from Dewan Chowdhury's observations, in parallel to the creation of fictional environments to engage adversaries within, there also exists the issue of how to handle nation-state actors who have agreed to the GGE norms of not-engaging critical infrastructure. Dave Aitel from Immunity proposed a partial solution to this problem in a March 2016 blogpost titled *A technical scheme for "watermarking" intrusions*.[8] His proposal would allow nation-states to share private keys and cryptographically sign

[6] Chowdhury, Dewan. *Hacking the Power Grid: Analyzing what Hackers do when they have access to the Power Grid Honeypot.* Fall 2015. http://www.malcrawler.com/4sics-powergrid-honeypot-presentation/

[7] "Threatpost. Power Grid Honeypots Puts Face on Attacks." Feb. 9, 20156. Accessed July 11, 2016. https://threatpost.com/power-grid-honeypot-puts-face-on-attacks/116217/

[8] Aitel, Dave. CyberSecPolitics. "A technical scheme for 'watermarking' intrusions." Mar. 8, 2016. Accessed July 11, 2016. http://cybersecpolitics.blogspot.com/2016/03/a-technical-scheme-for-watermarking.html

random data blobs within your intrusion chain such that defenders can attribute your activities with the help of their national cyber resources (who would have the commensurate private keys for validation).[9] The use of this type of active technique could at the very least deescalate response or retaliatory measures by nation-states on perceived attacks against national critical infrastructure resources, such as NPPs.

We also recognize that this third behavioral norm requires a shift in defensive thinking to engagement from passive observation and response. This shift to active cyber defense does not include hacking back or engaging adversaries outside of your own networks or computer systems. This behavioral norm requires NPP personnel to rethink their relationship with adversaries and carefully include in their portfolio of defensive capabilities mechanisms that allow for an increased level of controlled interaction.

VI. Conclusion

The gaps the INL has observed through our interactions with NPP operators and cyber defenders have allowed us to offer up these straight-forward cyber norms. In order for NPPs to bridge the knowledge gap between nuclear operations and cyber operations they will have to first, open their creative minds to consider the possibility that events and incidents may have a cyber origin, be thoughtful about exchanging what they learn with trusted community members, routinely engage in processes that exercise the formal and informal communication pathways that underlie competent response actions, and finally start to think about their relationship to their adversaries and how to engage them more proactively. Any organization that can take these behavioral norms and integrate them into their environment will have both the capacity to field a competent cyber defensive capability and the steady footing to shape their future capability acquisition process via expanded knowledge networks and inclusion of what is still considered non-traditional cyber defensive actions.

VI. Context

During the peer review process two helpful points were raised about this paper. The first was in relation to existing government initiatives that are promoting cyber threat education and information exchange. Within the United States there are a number of good initiatives such as Cybersecurity Information Sharing Act of 2015, the Department of Homeland Security US-CERT Critical Infrastructure Cyber Community (C Cubed), and the NIST Framework which all provide guidance and outreach for critical infrastructure providers. The majority of our engagements are internationally focused and while many nation states are interested in US best practices, the information does not flow as seamlessly as we would hope. So while US NPPs and CI providers may have easier access to these helpful programs, we do not generally see similar initiatives outside of the US. While our proposed norms are helpful both within the US and abroad, our problem space is almost entirely beyond US borders. The second point was with regards to how these behavioral norms align with the norms proposed by the UN GGE. The UN GGE norms provide some proscriptive boundaries with regards to critical infrastructure cyber security that we believe enables our behavioral norms that exist at the NPP and regulator level. It is our hope by connecting the two sets of norms that we are able to close the gap between what are aspirational nation state norms and practical NPP behaviors.

[9] Ibid.