CSCI 465 Net/App Security

Mia Weber

11/03/2023

Cybersecurity & Ethics Across the Globe

Cynthia A. Wright
Principal Cybersecurity Strategy and Policy
MITRE Corporation

Introduction:

Cynthia is a retired U.S. military officer with 25+ years in national security, cyber strategy, and policy, and in leading large organizations through strategic transformation initiatives.

MITRE is an organization that exists to give the best advice possible to governments regarding policy and technical development. Cynthia and MITRE support the US government without conflict of interest and do a lot of work with developing nations.

Daniels Fund Ethics Initiative Principles

Integrity – Act with honesty in all situations
Trust – Build trust in all stakeholder relationships
Accountability – Accept responsibility for all decisions
Transparency – Maintain open and truthful communications
Fairness – Engage in fair competition and create equitable and just relationships
Respect – Honor the rights, freedoms, views, and property of others
Rule of Law – Comply with the spirit and intent of laws and regulations
Viability – Create long-term value for all relevant stakeholders

Integrity

Act with honesty in all situations.

- Cynthia talked about her consultancy in the Balkans and discussed how her and her team had good partners and bad partners in this process. Bad partners wanted to exploit the client and made offers to locate vulnerabilities (not fix, just locate) for 24 million dollars.

Integrity means not acting on the temptation to exploit the fears of your clients. Often people will leverage recent attacks to charge exorbitant prices for a non-value added “service”.

? How many other organizations (non-government entities) does your team work with? Are there signs ahead of time that an organization might violate the integrity of the partnership?

Trust

Build trust in all stakeholder relationships.

UN Confidence-building Measures between countries to combat cyber crime

I. **Sharing, providing, and exchanging information** (warnings to others, even if it means exposing one's own failures)
   a. There is a misconception that sharing shows you are weak and don't know what you are doing, especially between regional competitors.

II. **Facilitating Communication** ("to prevent and reduce the risk of misperception, escalation, and conflict; and to clarify technical, legal, and diplomatic mechanisms to address ICT-related requests")
   a. Even getting people to trust each other within a government is challenging. People are quick to point fingers at another country when oftentimes an attack was from a botnet that the other country knows nothing about. The goal is to defuse miscommunications and increase communication.

III. **Enacting effective national legislation to enable bilateral cooperation in counterterrorism and criminal law matters**
   a. In many countries they have laws that tell you what you CAN do rather than what you CAN'T do ("default deny" vs "default allow"). We need National legislation in place that lets you share information with a neighboring country without fear of being prosecuted for treason.

IV. **Producing a consensus ICT security glossary** (common lexicon)
   a. Ukraine was switching the widely accepted meanings of "cyber security" and "cyber defense". What meant explicit offensive action to one party meant passive prevention to the other. What something means to one person doesn't guarantee that everyone has the same definition for that particular term.

V. **Promoting public-private partnerships** (important for governments with weak civil sectors)
   a. If many countries do work with AWS or Facebook, those private sector companies can be a bridge between governments. One country that Cynthia worked with had only 6 people working in a cyber operations department for the ENTIRE country, and she mentioned that this is not uncommon for their team to encounter.

VI. **Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident** (to normalize response actions across nations)
   a. Like corporate leadership, national leaders who don't "do" cyber also don't want to hear about cyber. We need to get countries to make commitments and actually financially invest and commit to those commitments.

VII. **Improving the security of national and transnational ICT-enabled critical infrastructure** (prevent incidents that affect civilians and/or national security)

VIII. Investigate the spectrum of cooperative measures to prevent and ICT-triggered conflict
   a. "Hey, before you start shooting, let's pick up the phone" also needs to be adapted for the cyber field too.

Accountability

Accept responsibility for all decisions.

Director of server security who had previously been convicted of selling information of previous clients. Walked it with an external drive and downloaded the registry of all the citizens of the country and sold it on the black market and kept his job with no repercussions.

We need to work harder to hold people accountable for their actions in the cyber space.

Transparency

Maintain open and truthful communications.

Africa: Facebook defacement is a top concern

- Tendency to embrace internet surveillance in developing nations, including spyware targeting journalists
- Internet shutdowns to block negative "press" about government actions

Cynthia mentioned that this happened primarily in Africa where governments tend to be unpopular and rely on force and intimidation to stay in power. In these situations, even minor cyber-attacks can make the government look weak.

- Because of this, the governments first reaction is to find out who was responsible for the attack and throw them in jail. In order to identify the guilty party, you have to see what is happening on private networks in the country.

A lot of Cynthia and her team's work in Africa has been informing governments how transparency and honestly with citizens often ends better than constant surveillance of your own people (China is a primary example).

Fairness

Engage in fair competition and create equitable and just relationships.

Corruption is a huge issue in the cyber space.

- Nepotism over qualifications (a big barrier to cyber success)
- Using compliance regulations as a weapon against your enemies (i.e., as an excuse to throw them in jail, get them fired, or fine them out of business)
- Oligarchs blocking CIP cybersecurity legislation because regulation might invite scrutiny/cut profits

Respect

Honor the rights, freedoms, views, and property of others.

Leading example is EU-GDPR (General Data Protection Regulation)

- Nepal: can't take or share a photo of an individual without permission

People have a right to maintain their own identities, data, and a presence on the internet and that right shouldn't be violated.

Cynthia talked about a colleague who got asked a question at a cyber convention about witchcraft and the internet. Her colleague had to both respect the views and beliefs of the person asking the question and clarify the misconception. The respect aspect is essential to all cyber discussions.

? You touched on data privacy, in a world where individual's right to their own data is still very much restricted, what are the "big steps" that need to happen in order to move towards comprehensive data ownership and security laws?

Rule of Law

Comply with the spirit and intent of laws and regulations.

Tallinn Manual – what is ok to do in a conflict and what is not ok?

- Modeled after the Geneva Convention (i.e., the right for a proportional display of self-defense after an attack).

Red Cross has proposed new rules for civilian hacktivists:

I. Don't direct cyberattacks against "civilian objects" like public services of infrastructure
   a. Means that if you can't guarantee that you won't impact a civilian object you shouldn't do it.
II. Don't use malware that spreads automatically
   a. You have to be able to track something and know what it will affect for it to be ethical.
III. When attacking a military objective, do whatever's possible to avoid the impact on civilians
IV. Don't attack medical or humanitarian targets
V. Don't attack targets that are "indispensable" for the survival for civilians, such as nuclear electrical generating stations
VI. Don't make violent threats to terrorize the population
VII. Don't incite others to violate international human law
VIII. Comply with the rules even if the enemy doesn't

Russian cyber-attacks being investigated as War Crimes; Ukraine "IT army (civilian hacktivists) have retaliated.

Viability

Create long-term value for all relevant stakeholders

- Positive: E-Gov efforts everywhere but in the US
  - The US gov isn't even here yet, but lots of other governments are.
- Positive: Focus on cyber workforce development
- Negative: Governments buying "sexy" cyber technologies at the expense of taking basic measures to protect their own citizens' data (i.e., "Dark Web Intelligence" vs unlicensed software hosting citizen data, critical services)

- Negative: Pirated software rife everywhere in developing nations' government networks and critical infrastructure providers

Reflection

Overall, I really enjoyed hearing what Cynthia had to say about ethics in cybersecurity. She covered all the bases of the Daniels Fund Ethics Initiative Principles in appropriate detail. Cynthia's job seems really amazing, but I couldn't imagine having to learn concerning and vulnerable aspects of a government's cyber program and then have to walk away knowing they might not take your advice and continue to make poor decisions about their national security. That being said, it is nice to learn more about some of the other job opportunities that exist for cyber professionals in the public sector and the government that are outside a strictly military space. This discussion was valuable and drew my attention to aspects of the cybersecurity industry that I usually take for granted. It was especially crazy to hear some of her stories of corruption and immorality that are rampant in governments around the world.