STATE-SPONSORED CYBER WAR: WHAT YOU NEED TO KNOW

ALBERT (BUZZ) SCHERR

PROFESSOR OF LAW

CHAIR, INTERNATIONAL CRIMINAL LAW & JUSTICE PROGRAM

UNH FRANKLIN PIERCE SCHOOL OF LAW

603-513-5144

ALBERT.SCHERR@LAW.UNH.EDU

INTERNATIONAL CRIMINAL LAW & JUSTICE PROGRAM

- Chat feature
- We are recording
- International Criminal Law & Justice Program
  - Masters & LLM degrees online
  - full & part-time
  - https://law.unh.edu/international-criminal-law-justice-program
- “When Does A Cyber Attack Count as a Declaration of War?”
  - https://unhlaw.podbean.com/e/cyber-war-1561134191/

INTRODUCTION: WHAT YOU NEED TO KNOW

1. Cyber attacks are happening & they're state-sponsored & intentionally destructive

2. Cyber attacks are happening on infrastructure

3. Cybersecurity efforts have improved & still lag behind

4. Potential damage is fundamentally different than other disasters
   - Scope
   - Duration
   - Intentionality
   - Unpredictability

CYBER ATTACKS ARE HAPPENING… 1

From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyber weapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

(https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?action=click&contentCollection=Middle%20East&module=RelatedCoverage&region=Marginalia&pgtype=article#story-continues-1)

CYBER ATTACKS ARE HAPPENING… 2

The Justice Department on Thursday unsealed an indictment against seven computer specialists who regularly worked for Iran's Islamic Revolutionary Guards Corps, charging that they carried out cyberattacks on dozens of American banks and tried to take over the controls of a small dam in a suburb of New York.

The indictment, while long expected, represents the first time the Obama administration had sought action against Iranians for a wave of computer attacks on the United States that began in 2011 and proceeded for more than a year, paralyzing some banks and freezing customers out of online banking.

[New York Times, 3/24/16; https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html#story-continues-1]

CYBER ATTACKS ARE HAPPENING… 3

In 2013, an unauthorized user from China hacked into the U.S. Corps of Engineers' National Inventory of Dams, a database of information on the vulnerabilities of major dams in the United States.

The database contained categories of dams based on the number of people that would be killed if the particular dam failed. No public evidence exists that the Chinese government was involved.

CYBER ATTACKS ARE HAPPENING… 4

In 2014, British-owned BAE Systems reported that a **“cyberespionage toolkit’”** known as Snake or Ouroboros had been found in the government computer networks of the Ukraine. The malware gave the hackers full remote access to the system, thereby enabling surveillance and data theft.

Based on a measure of evidence, the suspicion was that the hackers were Russian. Similar evidence had been found in systems in Lithuania, Britain and Georgia. Again, no public information exists that the Russian government was involved though the hacking in the Ukraine became known as what appeared to be Russian-inspired unrest in the Ukraine was growing.

….& THEY'RE STATE-SPONSORED

In a public statement in December, 2015, Ukraine's president, Petro Poroshenko, reported that there had been 6,500 cyberattacks on 36 Ukrainian targets in just the previous two months.

International cybersecurity analysts have stopped just short of conclusively attributing these attacks to the Kremlin, but Poroshenko didn't hesitate: Ukraine's investigations, he said, point to the "direct or indirect involvement of secret services of Russia, which have unleashed a cyberwar against our country."

To grasp the significance of these assaults—and, for that matter, to digest much of what's going on in today's larger geopolitical disorder—it helps to understand Russia's uniquely abusive relationship with its largest neighbor to the west.

Moscow has long regarded Ukraine as both a rightful part of Russia's empire and an important territorial asset—a strategic buffer between Russia and the powers of NATO, a lucrative pipeline route to Europe, and home to one of Russia's few accessible warm-water ports. For all those reasons, Moscow has worked for generations to keep Ukraine in the position of a submissive smaller sibling.

Yushchenko, who ended up serving as Ukraine's president from 2005 to 2010, believes that Russia's tactics, online and off, have one single aim: "to destabilize the situation in Ukraine, to make its government look incompetent and vulnerable."

He lumps the blackouts and other cyberattacks together with the Russian disinformation flooding Ukraine's media, the terroristic campaigns in the east of the country, and his own poisoning years ago—all underhanded moves aimed at painting Ukraine as a broken nation.

"Russia will never accept Ukraine being a sovereign and independent country," says Yushchenko, whose face still bears traces of the scars caused by dioxin toxicity. "Twenty-five years since the Soviet collapse, Russia is still sick with this imperialistic syndrome."

But many global cybersecurity analysts have a much larger theory about the endgame of Ukraine’s hacking epidemic: They believe Russia is using the country as a cyberwar testing ground—a laboratory for perfecting new forms of global online combat. And the digital explosives that Russia has repeatedly set off in Ukraine are ones it has planted at least once before in the civil infrastructure of the United States.

…& INTENTIONALLY DESTRUCTIVE

Russia's hacking of 2016 election

- Russians purchased ads on YouTube, gmail and other platforms
- Significant fake presence on Twitter
- Acquisition of e-mails from Democratic & Republican parties
- Hacking into election mechanisms in states and counties

THE JOINT INTELLIGENCE REPORT

- We assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks.

  - Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.

- We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes.

- We assess Russian intelligence services collected against the US primary campaigns, think tanks, and lobbying groups they viewed as likely to shape future US policies. In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016.

    - The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. We assess that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.

- Public Disclosures of Russian-Collected Data.

- We assess with high confidence that the GRU used the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to release US victim data obtained in cyber operations publicly and in exclusives to media outlets.
  - Content that we assess was taken from e-mail accounts targeted by the GRU in March 2016 appeared on DCLeaks.com starting in June.

- We assess with high confidence that the GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks.

- Russian Cyber Intrusions Into State and Local Electoral Boards.
- Russian intelligence accessed elements of multiple state or local electoral boards. Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment.

- DHS assesses that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying.

- We assess the 2016 influence campaign reflected the Kremlin's recognition of the worldwide effects that mass disclosures of US Government and other private data—such as those conducted by WikiLeaks and others—have achieved in recent years, and their understanding of the value of orchestrating such disclosures to maximize the impact of compromising information.

INDICTMENTS

- Individuals & companies in St. Petersburg, Russia

- Name-and- shame Indictments only
  - Extradition Issues
  - Evidence-gathering issues

- Note The problem with managing cyber attacks through the criminal justice system

CYBER ATTACKS ARE HAPPENING ON INFRASTRUCTURE

- Russian hacking of 2016 election process was an attack on a kind of infrastructure

- In early 2007, the Baltic nation of Estonia was well on the way to earning its recently acquired nickname, “eStonia”: the country had used computer networks to automate and integrate nearly every aspect of its governance and society.

- Estonian citizens banked, voted in parliamentary elections, and even paid for parking using interconnected computer systems. The internet phone company Skype headquartered there. The nation was a veritable utopia of the burgeoning internet culture and a “window into the future.”

- All of that changed on April 27, 2007, when the nation suffered what was then the most widespread cyber attack in history, and possibly the first instance of international cyber war.

- In only a few hours, the nation's media websites, banking sites, and government computers all suffered black outs. Attackers targeted all of Estonia's major commercial banks, telecoms, media outlets, and some essential servers.

- Using Distributed Denial-of-Service (DDos) attacks, the assaults lasted twenty-two days and effectively crippled the nation's electronic infrastructure.[8] By flooding the Estonian computer systems with an enormous number of requests, the attackers were able to effectively overload the systems and thereby deny service to legitimate users. Nearly every Estonian citizen felt the impact, and the populace reacted with hostility. Rioting and social upheaval followed. The unrest resulted in one death and injuries to 150 people.

AND … "HACKING GROUP TARGETING U.S. ELECTRIC UTILITIES" (6/14/19 REPORT)

"Xenotime, a group of hackers that has previously targeted oil and gas companies, has been targeting the U.S. electric grid in recent months, according to new research released Friday by cybersecurity group Dragos. Dragos reported that the Xenotime group began "probing" the networks of electric utilities in both the U.S. and countries in the Asia-Pacific region in late 2018.

The report noted that none of the probes resulted in the group gaining access to an electric utility's system, but wrote that "the persistent attempts, and expansion in scope is cause for definite concern."

(https://thehill.com/policy/cybersecurity/448587-hacking-group-targeting-us-electric-utilities-report)

CYBERSECURITY EFFORTS HAVE IMPROVED & STILL LAG BEHIND

- Private industry has significantly ramped up its cybersecurity efforts
  - Raytheon and battery-pack testing story

- Education: cybersecurity Masters and PhD programs at educational institutions are growing dramatically over the past 5 years.

  Both technical & policy degrees

- . The U.S. Cyber Command, the NSA and the Department of Energy among others have significantly increased their efforts in this area.

CYBERSECURITY EFFORTS HAVE IMPROVED & STILL LAG BEHIND

- The problem: " some have suggested that the cyberattacks that crippled power distribution centers in Ivano-Frankivsk region of Western Ukraine in 2015 preyed on systems that "were surprisingly more secure than some in the US, since they were well-segmented from the control center business networks with robust firewalls."

(Ken Zetter, "Inside The Cunning, Unprecedented Hack of Ukraine's Power Grid," 3/3/16, *Wired, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid0)*

POTENTIAL DAMAGE IS FUNDAMENTALLY DIFFERENT THAN OTHER DISASTERS

- Scope
- Duration
- Intentionality
- Unpredictability

SCOPE

- A power-grid apocalypse is different than a natural disaster

- “A region-wide, intentional and systematic effort to disable power grids has the potential to be a longer -lasting event than an extreme weather event. It presents a more comprehensive disabling of infrastructure of all sorts …. “

(Robert Walton, “Lloyds: Cyber attack on US power grid could cost $1 trillion,” 7/17/15, *Utility Dive, https://www.utilitydive.com/news/lloyds-cyber-attack-on-us-power-grid-could-cost-1-trillion/402454/*)

SCOPE

(1) The loss of the provision of health care, home heating, air conditioning, schools, employment circumstances public safety;

(2) The loss of the ability to communicate by landline, the internet, cellphones;

(3) The complete disruption of the region or country's micro- and macro-financial systems like electronic bill payment; electronic money transfers between individuals and businesses as well as the complete shutdown of the banking system; the stock market; the Federal Reserve.

4) The loss of ability to manage gas and oil flow as both systems now depend on computers to mange that flow.

5) Consider whether the power grid attack temporarily disables computers or completely ruins them

DURATION

- A Lloyds of London modeling of the disabling of the power grid in 15 states on the eastern seaboard, including New York City and Washington, D.C., suggests that such an event might leave 93 million customers without power. Evacuation on that scale is more than a bit challenging, if even possible."

- Depending on the time of year, extreme cold or heat could result in thousands of deaths over a longer period of time

(Robert Walton, "Lloyds: Cyber attack on US power grid could cost $1 trillion," 7/17/15, *Utility Dive, https://www.utilitydive.com/news/lloyds-cyber-attack-on-us-power-grid-could-cost-1-trillion/402454/)*

INTENTIONALITY

- “This month (March ‘19), the U.S. government revealed its concerns about Russian incursions into the operating systems of domestic electric power plants and noted that the efforts to disrupt date back to 2013. These attacks have the capability to bring down all or part of our electricity service...

- Such large-scale grid cyberattacks were foreseen. The Departments of Energy and Homeland Security identified the grid’s vulnerability to cyberattacks some time ago and called for new protective measures in the DOE-led January 2017 Quadrennial Energy Review…

- The study, which analyzed the entire U.S. electricity system, noted that that the key critical infrastructures underpinning the nation’s economy and national security — transportation, water, finance, natural gas, oil, communications/IT — depend upon a reliable electricity “uber-network.”

(https://thehill.com/opinion/energy-environment/379980-us-power-grid-needs-defense-against-looming-cyber-attacks)

UNPREDICTABILITY

- When the cyber attack on the power grid would occur is much more a function of international events than any natural disaster.

- And … when the cyber attack on the power grid would occur is much more a function of who controls the governmental systems in this and in other countries

FOR EXAMPLE …

- United States Cyber Command on Thursday conducted online attacks against an Iranian intelligence group that American officials believe helped plan the attacks against oil tankers in recent weeks, according to people briefed on the operation.

- The intrusion occurred the same day President Trump called off a strike on Iranian targets like radar and missile batteries. But the online operation was allowed to go forward because it was intended to be below the threshold of armed conflict — using the same shadow tactics that Iran has deployed.

(https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html?action=click&module=Top%20Stories&pgtype=Homepage)

OR …

- “The United States is stepping up digital incursions into Russia’s electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cybertools more aggressively, current and former government officials said…

- Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from the Department of Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States.

- But it also carries significant risk of escalating the daily digital Cold War between Washington and Moscow.

- But now the American strategy has shifted more toward offense, officials say, with the placement of potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before. It is intended partly as a warning, and partly to be poised to conduct cyberstrikes if a major conflict broke out between Washington and Moscow…

- Pentagon and intelligence officials described broad hesitation to go into detail with Mr. Trump about operations against Russia for concern over his reaction — and the possibility that he might countermand it or discuss it with foreign officials, as he did in 2017 when he mentioned a sensitive operation in Syria to the Russian foreign minister…

- Because the new law defines the actions in cyberspace as akin to traditional military activity on the ground, in the air or at sea, no such briefing would be necessary, they added."

(https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20Stories&pgtype=Homepage)

THE MORAL OF THE STORY

- Prepare!

LINKS ETC

- International Criminal Law & Justice Program
  - Masters & LLM degrees online
  - full & part-time
  - https://law.unh.edu/international-criminal-law-justice-program

- “When Does A Cyber Attack Count as a Declaration of War?”
  - https://unhlaw.podbean.com/e/cyber-war-1561134191/

- Albert (Buzz) Scherr

  Professor of Law & Chair, International Criminal Law & Justice Program

  UNH Franklin Pierce School of Law

  603-513-5144

  Albert.scherr@law.unh.edu