

SY403 – Third Short Exercise (17 September 2019)

The cybersecurity exercise you will build on Short Exercise One's introduction of an analytical discipline known as "serious discovery gaming." As before, this particular serious game will employ a cybersecurity vignette, with the goal of gaining insight into the:

- Key issue(s) and their root causes
- Primary stakeholders, their equities, and the relationships between them
- Possible solutions and their associated costs, incentives, and impediments

The scenario is set in the Spring of 2021. The scenario postulates a set of events that force the US to deal with an emerging cybersecurity crisis that plays out in the domain of space (recall that the US DoD holds that there are five domains of interest: Air, Land, Sea, **Space** and Cyberspace...)

In response to the crisis the President convenes a meeting of cybersecurity experts from across government, industry, academia, and interest/advocacy groups to develop recommendations for addressing the multi-tiered problems exposed by the crisis. **As a White House Fellow, you made the cut ☺**

The National Security Advisor, who will be played by your professor, will chair the meeting. You will be briefed on the cybersecurity situation and given guidance and tasking for your deliberations. The group will then divide into two or three teams (your instructor will make team assignments) to explore the problem and seek possible solutions.

The whole group will then reconvene to hear and discuss the best solution(s) each team has to offer.

Some of the key elements of the game are:

- Role playing - You are encouraged to speak to the issues, concerns, and ideas from your perspective.
- Multiple Functional Perspectives — We will cover several functional areas, each of which will consider cybersecurity through the lens of one functional perspective (various instruments of power... not just military).
- Multiple Disciplinary Perspectives – The best answers are always derived from teams comprised of people with different backgrounds and skill sets.
- Multiple Criteria – **Integration** will matter. Addressing one perspective or addressing the desires of only one stakeholder, totally at the expense of the others, is unlikely to produce the best solution.
- Multiple Candidate Solutions — You will likely consider and assess several possible solutions, and then identify the most promising one.
- Multiple Performance Measures - You should have in mind a number of measures-of-performance against which to assess the viability of solutions. These will be:
 - How well a solution alleviates the problem
 - How it impinges on stakeholder equities (all stakeholders should be defined and considered)
 - How costs and benefits are distributed
 - How effective incentives might be, and
 - How resilient the impediments will be in preventing the changes you recommend.

As with all analytical gaming, the success of the game (and value you derive from it) will be directly proportional to your personal engagement.

Exercise Background:

It is now the spring of 2021, nearly 24 months after the standup of the new US Space Force, which has largely been instantiated in the form of a Unified Combatant Command, referred to throughout this exercise as “US Space Command” or USSPACECOM.

1. The Crisis:

- a. The Defense Information Systems Agency (DISA) and the Air Force Chief Information Officer have detected a large-scale exfiltration of sensitive data from US Space Command (USSPACECOM) beginning in late May 2021.
- b. The complete set of losses are still unknown
- c. The USSPACECOM mission requires that its assets continue to be deployed around the world to support both military and civilian requirements.
 - i. Military dependencies on the data believed to be disclosed cut across all missions, all systems.
 - ii. Civilian dependencies on the data believed to be disclosed include the use of government systems (e.g., GPS) for applications from timing, geolocation, and navigation.
- d. Of note, government and private security specialists continue to investigate the spear-phishing campaign and subsequent breach of Defense Industrial Base (DIB) networks, it is still unclear what types of data were stolen or potentially compromised, who the attackers were, and if the attackers were able to access any additional systems via undiscovered connections.
- e. **Worst case assumption:** The compromised data could allow adversaries the means to gain privileged access to USSPACECOM systems (to include GPS and USSPACECOM Command and Control).

2. What we know about the attack vector:

- a. The spear-phishing campaign on DIB entities and was executed via a backdoor deployed on desktop computers awaiting patches for recently-discovered security vulnerabilities
- b. **While patches are available, they have not been widely deployed. The nature of the security vulnerabilities they ‘fix’ have been closely held by the intelligence community** owing to three factors:
 - i. the sources and methods involved in their discovery;
 - ii. the fact that they are also used by NSA, CIA and USCYBERCOM in the conduct of their offensive missions; and
 - iii. the danger that their public disclosure will open an immediate window of vulnerability for affected systems).

3. Immediate Response to the technical cyber aspects of the situation have been provided by:

- a. A third-party (private contractor) crisis response team hired by ERT LLC¹, a subcontractor for USSPACECOM with key mission projects in satellite and navigation technology.

¹ **NOTE!!!!** ERT LLC, a defense contractor with projects focused on satellite deployment, advanced navigation technology, and future system implementations, has been a growing firm within the DIB. Given the success it has had delivering on smaller yet critical technology-focused DoD mission priorities, the company has expanded its footprint within the armed services, requiring it to hire a greater number of analysts, programmers, and systems

- b. A USSPACECOM advanced computer incident response and digital forensics team will support the investigation, but these activities often take time and resources. Once the appropriate authorities receive and analyze the necessary technical information, more details will be provided about the confidentiality, integrity, and availability of the affected data and information systems
- c. Separately, USCYBERCOM has augmented a Cyber Protection Platoon that is dedicated to the support of the sustained defense of USSPACECOM systems.

4. Concerns regarding criticality:

- a. These attacks pose a significant threat to the US as reliance on GPS by military, industry, and the American public continues to grow.
- b. The President will need to take swift action in order to appear strong on defense and capable of supporting industry and the public during such times of uncertainty.
- c. However, with insight into the range of dependencies that can be delivered by GPS, a concerted effort to understand all potential attackers, vectors, and impacts of a response is critical.

5. Current Geo-political climate -- while many possible causes of this particular spike in cyber theft are possible, the US Intelligence community briefs the President on the following as the most promising explanation:

- a. Recent intelligence reporting has highlighted rising tensions on the Indian subcontinent.
 - i. Election of Prime Minister Narendra Modi's hardline, nationalist successor Geeta Vadlamannati.
 - ii. Increased concern of unprovoked incidents along the India-Pakistan border in the Kashmir region.
 - iii. 20th anniversary of the Kargil War approaching, intelligence analysts are closely watching memorial services on both sides of the border for any possible escalations or confrontations.
 - iv. Adding to the instability, US drone deployments over Pakistan have increased over the last decade (including "drone swarm" tactics), angering much of the Pakistani population.

b. Space race in South Asia:

- i. China's successful anti-satellite weapons test in 2007
- ii. Indian policymakers have recognized the need for a comprehensive space policy and an independent space situational awareness capability.
- iii. India is focused on improving remote imaging and sensing capabilities, communication capabilities, and positional and navigational capabilities.
- iv. India has successfully launched seven satellites into orbit, putting into place a proprietary satellite-based navigation system known as the Indian Regional Navigation Satellite System (IRNSS). Several factors led India to establish the IRNSS:
 - 1. Including denied access to the highly accurate US military GPS system

administrators. To meet demand, especially when it comes to staffing at its large network of data centers, ERT LLC has leveraged the H1B visa program for specific occupational series.

2. Lack of a formalized contract between India and US service providers for GPS
3. Before IRNSS, India relied on Russia's GLONASS system
4. Newly-elected Indian Prime Minister Vajpayee celebrated the IRNSS as a significant step forward for India's autonomy in the world.
5. Vowed to have IRNSS eventually replace the US GPS system and allow for both civilian and military use of the IRNSS by making it "more advanced than anywhere else on Earth."
6. Aerospace engineers have noted that the IRNSS system produces large errors due to the large height difference between the Himalayas (height of 8,000 meters) and the Indian Ocean (depth of 4,000 meters).
7. India has attempted to correct its GPS signals though accuracy is still a problem.
8. Pakistan's dominance over India in C4ISR is large and increasing.
9. Pakistan's military continues to be the only armed forces with access to the BeiDou Navigation Satellite System, China's proprietary navigation system, and coordination between the two nations on GPS technology appears to be increasing.

v. In particular, China has granted Pakistan's armed forces access to BeiDou's military services, previously only available to China's People's Liberation Army.

- vi. China has invested in a network of stations and receivers throughout Pakistan. Furthermore, to widen the geographic area, improve accuracy/performance.
- vii. China is nearing completion of its goal to launch 30 new, non-geostationary to replace geostationary which will offer complete coverage of the globe by 2020.
- viii. With three nuclear powers, China, Pakistan, and India, in close proximity to the Kashmir region, the Intelligence Community continues to monitor the situation and will provide updates in the event that there are any linkages with this case.

ix. As strategic alliances with both India and Pakistan have grown increasingly important for US foreign relations, both in civilian and military contexts, the current case of information theft from an USSPACECOM subcontractor could place US satellite assets in jeopardy.

- x. **Analysts cannot rule out responsibility for the recent data theft by either Pakistan or India as well as other states with interest in GPS advancements and geopolitical dynamics.**
- xi. Established agreements with other navigational services may require the US to engage in bilateral or multilateral coordination with other potentially affected entities or technologies.

Appendix 1: Background Information

1. Historic Precedents (illustrative) that offer understanding of previous US Government

Action(s):

- a. Chinese government theft of intellectual property: 2006-present day: Massive amounts of data related to defense systems, health records, welfare recipients, trade negotiations, critical infrastructure investments. Federal networks have also been a prime target in their own right, and a means for accessing industry knowledge held by the federal government.
- b. Operation Buckshot Yankee: 2008: The Department of Defense discovered a worm originating from a thumb drive used at US military bases in the Middle East. After infecting US military networks, this worm scanned computers for data, opened backdoors, and communicated with remote command and control servers. Attributed by some to the nation state of Russia.
- c. Rolling Tide: 2013: Intrusions into Navy and Marine Corps networks allegedly attributed to actors associated with the Iranian government.
- d. Snowden: 2013: Copied between 50,000 and 200,000 highly-classified documents and shared them with the press for public release leading to public outrage, international condemnation, asset compromises, and additional regulations.
- e. North Korean hack of Sony Pictures: 2014: North Korea executed a denial of service and ransomware campaign against Sony Pictures in 2014, in an attempt to compel Sony Pictures to cancel release of a film unfavorable to Kim Jon Un.
- f. PRC hack of Office of Personnel Management (OPM) in 2015: Government Accountability Office reports indicated that more work is needed to prevent future extraction.
- g. North Korean 2017 execution of a widespread ransomware attack on private and public networks (Wannacry)
- h. Russian (GRU) attack on Ukrainian government (via medoc) in 2017: spills into private sector (as notPetya) causing hundreds of millions of dollars in losses.

2. Information on the Victim: US Space Command:

- a. The newest of the Combatant Commands (sometimes errantly referred to as the “Space Force”)
- b. USSPACECOM supports US military operations worldwide through the use of satellite, launch, and cyber operations (both defensive and offensive).
- c. Provide space and cyberspace capabilities to the Joint Force and the nation through direct and/or indirect support.
- d. Make the space domain reliable to combat forces via the launch of satellites and other high-value payloads, ISR and Navigation
- e. Operational division for development of cyber tactics, techniques, and procedures in support of information operations, combat communications, and network warfare.
- f. Global Positioning System (GPS) Directorate within the Space & Missile Systems Center has been a high-value target for adversaries given its responsibility for the constellation of orbiting satellites that provides navigation data to military and civilian users
- g. Facts on GPS:

- i. US Global Positioning System satellites orbit emitting navigation signals
- ii. Additionally, GPS provides two different service levels, Standard Positioning Service (GPS-SPS), available to civilian users, and Precise Positioning Service (GPS-PPS), available to US military users.
- iii. In the past, the US government possessed the ability to degrade the accuracy of GPS-SPS, through a process known as Selective Availability.
- iv. In 2000, President Bill Clinton ended this practice and the US has no intention to use it again.
- v. While the accuracy of GPS-SPS and GPS-PPS are equal, GPSPPS provides other advantages, including enhanced security, jam resistance, and ionospheric correction.
- h. Advanced navigation capabilities, first developed by the DoD in 1972, have increased in their impact on both military and civilian life.
- i. During Operation Iraqi Freedom in 2003, the GPS satellite constellation allowed the delivery of 5,500 GPS-guided Joint Direct Attack Munitions with pinpoint precision
- j. GPS continues to fill a crucial role in air, ground, and sea operations guiding countless service members and equipment to ensure they are on time and on target.
- k. USSPACECOM continues to refine capabilities by improving accuracy, dependability, and longevity of our satellites and ground systems.
- l. By granting access to GPS-SPS for non-military entities, the US government has developed a robust engagement effort with international counterparts including Russia, India, and the European Union to coordinate development and execution of their respective systems.
- m. Furthermore, the proliferation of mobile devices today has also spurred a rise in location-based metadata collected by service providers.

3. Industry playing a growing role in national defense via public-private partnerships

- a. Increasingly critical to the Nation's defense apparatus
- b. Such collaboration is evidenced in disaster recovery, cyber defense, and in-theater combat support.
- c. DoD has a long history of coordination with innovative companies including the creation of advanced tools, implementation of data sharing frameworks, and development of new IT architectures.
- d. In recognition of potential risks posed by a growing number of contractors engaged with DoD entities, DIB companies and DoD stood up the DC3 to serve as an operational hub for information assurance and information sharing in order to safeguard intellectual property and disseminate analysis, diagnostics, and mitigation strategies across the mission environment.
- e. Executive Branch has released several key directives for Federal agencies as well as government contractors to ensure that sensitive information is protected from theft, exploitation, and other potential compromises.

4. Guidance on Data Theft

- a. Advanced navigational equipment has become ubiquitous in modern society and loss of such tools could compromise US interests in maintaining peace in volatile regions and in ensuring economic growth. In fact, the current case has already led several

multinational corporations to raise their alert levels through CIO and CISO channels to avoid further instances of intrusions into their networks and potential losses of consumer confidence.

- b. The US Executive Branch has established directives that seek to promote greater information security protocols in both the public and private sectors (to include improving resilience, information sharing and accountability).
 - i. Both have been slow to stand up the necessary programs to prevent data theft, which often require extensive coordination as well as appropriate communication and waiver of certain expectations of privacy from employees.
 - ii. As a result, no two agencies or companies are in the same place in their maturity and sophistication.
- c. The private sector is caught in the middle In the case of any dual-use technologies, industry is often operating at the direction of governments who seek to leverage such capabilities for a variety of purposes.
- d. For purposes of the exercise, you may assume that USCYBERCOM has standing orders to defend the Defense Industrial Base of the US, to include both facets of its 2018 doctrine, "Persistent Engagement" and "Forward Defense".

Appendix 2: Defense Industrial Base Contractor Breach Notification sent to Department of Defense Official

10 May 2021

FLASH PRECEDENCE

SUBJECT: Loss of confidence in critical system(s)


To: General Siber Wannabee, USAF, Commander US Space Command

From: Jonathan Griswold Chief Executive Officer ERT LLC

1. Pursuant to National Industrial Security Program instructions, I am notifying you of a breach of security in late May 2021 involving classified information housed on protected ERT LLC networks.
2. After initiating a preliminary inquiry, we discovered that **unknown actors targeted classified information contained on MAC I systems**. Additionally, this inquiry found that the classified information was transmitted to foreign IP addresses. A computer incident response and digital forensics team is currently investigating the specific circumstances surrounding the loss, and an initial report will be submitted in two weeks. **The consequences of loss of integrity or availability of a MAC I system could include the immediate and sustained loss of mission effectiveness for US Space Command and the broader defense apparatus**. Moreover, given the integration of defense technology into civilian applications, second- and third-order effects could be felt by the general public as well. As outlined in our approved incident response plans, we have activated a crisis response team and contacted appropriate authorities as well as mitigation experts. We will continue to keep you apprised of our actions to address this incident and will send an updated report for your review as soon as possible.

Appendix 3: Pastebin Posting:

The below was pasted in the popular data dump site *pastebin.com* <http://pastebin.com/brasLH26>

 Untitled

A GUEST JUN 26TH, 2019 101 NEVER

text 0.16 KB raw download clone embed report print

1. By Pak H4ckrz
2. We have stolen information on your Space capabilities. All your Satellites belonging to us now.. control of your DroneS is in our hands.. We will swat them from the Sky like flies.
3. Now American drone Strikes on innocent Pakistanis will not Be Tolerated anymore..
4. Here Is Example Info.. To Prove:
- 5.
6. 139.0°W Americom-8 Lockheed MartinA2100A US SES Americom &AT&T Alascom Television and radio broadcasting 24 C band(Canada,Caribbean,CONUS) 19 December 2000,Ariane 5G Previously GE-8 for GE Americom; also known as Aurora III; replaced Satcom C-5 in March 2001 11/20/2008
7. 137.0°W Americom-7 Lockheed MartinA2100A US SES Americom Television and radio broadcasting Canada,CONUS,Mexico 14 September 2000,Ariane 5G Previously GE-7 for GE Americom 11/20/2008
8. 135.0°W Americom-10 Lockheed MartinA2100A US SES Americom SWE 11/20/2008 Canada,Caribbean,CONUS,Mexico 5 February 2004,Atlas II-AS
9. 129.0°W Galaxy-12Orbital Sciences CorporationStar-2 US Intelsat Television/Radio Broadcasting 9 April 2003, Ariane 5G 123.0°W replaced failed Galaxy 15
10. 131.0°W Americom-11 Lockheed MartinA2100A US SES Americom Television and Radio Broadcasting 24 C Bandtransponders(Canada,Caribbean,CONUS,Mexico) 19 May 2005, Atlas II-AS 11/20/2008
11. 129.0°W Galaxy-27FS-1300 US Intelsat Television broadcasting & Satellite Internet Access 25 September 1999,Ariane 44LP Formerly known as IA-7 and Telstar-7 11/20/2008
12. 127.0°W Galaxy-13HS-601 US Intelsat 24 C Bandtransponders 1 October 2003,Zenit-3SL Same satellite as Horizons-111/20/2008
13. 127.0°W Horizons-1 HS-601 US Japan Satellite Systems 24 Ku-Bandtransponders 1 October 2003,Zenit-3SL Same satellite as Galaxy-13 11/20/2008
14. 125.0°W Galaxy-14Orbital Sciences CorporationStar-2 US Intelsat 24 C Bandtransponders- North America 13 August 2005,Soyuz-FG/Fregat 11/20/2008
15. 123.0°W Galaxy 18LS-1300 US Intelsat Television and radio broadcasting North America 21 May 2008, Zenit-3SL Hybrid C/Ku-band satellite 11/19/2008
16. 121.0°W Galaxy-23FS-1300 US Intelsat Direct Broadcasting North America 7 August 2003,Zenit-3SL Hybrid C/Ku/Ka-band satellite; C band payload referred to as Galaxy-23 11/26/2008
17. 121.0°W EchoStar-9 FS-1300 US Echostar/DISH Network Direct Broadcasting North America 7 August 2003,Zenit-3SL Hybrid C/Ku/Ka-band satellite; Ku/Ka-band payload referred to as EchoStar-9 11/26/2008
18. 119.1°W DirecTV-7S LS-1300 US DirecTV Direct Broadcasting 54 Ku-bandtransponders 4 May 2004, Zenit-3SL 8 active transponders at this time 11/26/2008
19. 118.8°W EchoStar-7 Lockheed MartinA2100AX US Echostar/DISH Network Direct Broadcasting 32 Ku-bandtransponders 21 February 2002,Atlas IIIB 21 active transponders at this time 11/26/2008
20. 115.2°W XM-Blues US 30 October 2006,Zenit-3SL
21. 110.0°W EchoStar-11 LS-1300 US Echostar/DISH Network Direct Broadcasting 17 July 2008, Zenit-3SL 11/19/2008
22. 110.0°W EchoStar-10 A2100AXS US Echostar/DISH Network Direct Broadcasting 15 February 2006,Zenit-3SL
23. 110.0°W DirecTV-5LS-1300 US DirecTV Direct Broadcasting 7 May 2002, Proton 32 Ku-bandtransponders
24. 105.0°W AMC-18 A2100A US SES Americom Direct Broadcasting Canada,Caribbean,CONUS,Mexico 8 December 2006,Ariane 5

Appendix 4: Judging Criteria

Student recommendations will be judged using the following five categories.

- a. Understanding of Cyber Policy
 - a. The team demonstrated a superior knowledge of cyber conflict policy issues, accurately named specific actors, and applicable instruments
 - b. The team demonstrated a comprehensive knowledge of cyber conflict policy issues, identified appropriate actors, and instruments
- b. Identification of key issues
 - a. The team successfully identified and fully responded to critical cyber conflict policy issues posed by the scenario
 - b. The team identified and responded to the main policy issues posed by the scenario
- c. Analysis of policy response alternatives
 - a. The team's suggested policy response alternatives effectively addressed the scenario, and the team thoroughly analyzed the tradeoffs involved with other policy alternatives
 - b. The team's suggested policy response alternatives only partially addressed the scenario and/or some sections lacked sufficient analysis or justification
- d. Structure and Organization
 - a. The team clearly and concisely presented policy response alternatives and fully communicated the analysis supporting their recommended response and all alternatives
 - b. The team effectively presented their policy response alternatives and recommended response, but did not fully communicate the analysis of alternatives and/or justification of their recommended response
- e. Originality and Creativity
 - a. The team offered original, creative, and innovative solutions to the scenario that go beyond existing canonical cyber conflict policy literature
 - b. The team exhibited a distinctive approach to the scenario, but largely drew on well known solutions