NESA SENIOR EXECUTIVE FORUM
"Cybersecurity, Supply Chains, and the Digital Stack"

13-17 April 2026
Final Report

NEAR EAST SOUTH ASIA (NESA) CENTER FOR STRATEGIC STUDIES
POC: Jeffrey Payne, NESA; jeffrey.payne.civ@ndu.edu

BLUF:
NESA conducted a Senior Executive Forum from 13-17 April that featured 50 participants from 32 partner nations for conversations designed around how cybersecurity and other aspects of emerging technology is shaping the future of national security across domains. Participants received training on how the U.S. is developing its approaches to seizing technology to enhance its own capabilities and how that process facilitates means for partners to contribute. Topics discussed in detail include how AI is being integrated into operations, how public-private partnerships are facilitating new means for quick adoption of key tools, how cybersecurity is evolving and what threats pressure our existing cyber infrastructure, and how technology informs military and security doctrine, among others. Participants also took part in a tabletop exercise designed around how various components of a cybersecurity crisis emerge, are addressed, and further resiliency achieved.

Key insights revealed through the week-long program include:

- The transformation in how government can steer technology policy amidst a period of intense innovation is not settled and a source of concern. The transition from a state-centric system to one of public-private interdependence within the U.S. is a process that is not necessarily a preferred option everywhere. More must be done in facilitating, educating, and familiarizing partnering states with policy options and means of plugging in with one another.

- Sovereignty is a concern when it comes to technology policy options, given the current form of technological innovation globally and pressure building on bureaucratic structures. The digital sovereignty discussions are not settled around the world. Future partnerships on technology, especially with private sector actors, should include mechanisms for tailoring innovation with existing policy and how auditing the reliability of technology can be structured into agreements.

- Competition between the U.S. and China in technology is not going to disappear (and may well intensify in specific sectors). As such, geopolitical considerations cannot be extracted from the building, altering, or certifying of technology policy by any state.

- Participants routinely detailed worries over the blurring of traditional categories of national security threats based upon the digital domain. Existing bureaucratic structures may not be sufficiently positioned to address such threats.

- Public-Private partnerships in technology may be a model for adopting technologies by government structures, but the influence private sector firms have over such discussions remains an open question. Innovators from the private sector can move at a pace and scale that few governments can match, but private interests do not necessarily align with the public interests that governments serve. As such, consideration over how private sector interests are inserted into public policy will remain a priority.

- The tabletop exercise showed acceptance of a whole-of-government approach to escalating cyber crises. One poignant point of emphasis made by many of the participants was the necessity of retaining the ability to communicate with the public during a crisis. Effective government responses to a crisis cannot purely be focused upon alleviating the threats present, but also in keeping the public informed over the status of government operations and the restoration to any damaged digital infrastructure.

- Finally, the NESA team compiled a direct listing of lessons learned from the overall event:
    - Develop allied access agreements for compute, the cloud, and data.
    - Cybersecurity threats are difficult to attribute to a particular actor and the cloudiness of the digital realm makes it a continuous nexus for various forms of criminality (from hacks, theft, to laundering).
    - Verifiable trust mechanisms (supply chain assurance, code transparency) are in demand.
    - The speed of innovation can outpace governance.
    - Non-state actors, particularly large technological firms, are a stakeholder in global technology policy.

PROGRAM AGENDA:

Monday, April 13, 2026

0800 – 1000 **Arrival – VCC Registration**
(Participant Introductions)

1000 – 1015 **Course Director's Welcome and Introduction**
Jeff Payne, *Assistant Professor, NESA Center for Strategic Studies*

1015 – 1030 **Dean's Welcome**
COL (ret) Richard Wiersema*, Academic Dean, NESA Center for Strategic Studies*

1030 – 1200 **Session 01: A Brave New World – Emerging Technology in Warfare**
Moderator: ***Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speakers:

- ***Admiral James Foggo****, U.S. Navy (ret.), Dean, Center for Maritime Strategy*
- ***LTG (ret) Terry Wolff****, Distinguished Professor, NESA Center for Strategic Studies*

1200 – 1230 **Group Photo Break (Marshall Hall Atrium)**

1230 – 1330 **Lunch**

1330 – 1445 **Session 02: Risk Assessment and Digital Connectiveness**
Moderator: ***Fahad Malaikah****, Professor of Practice, NESA Center for Strategic Studies*
Speakers:

- ***Dr. Nikita Shah****, Senior Fellow, Intelligence, National Security, and Technology Program, CSIS*

1445 – 1500 **Tabletop Exercise Briefing**
All participants will take part in a series of breakout sessions throughout the week that rely on your respective experiences and calculations as it relates to the larger issue of technology in contemporary national security and warfare. The sessions will be designed around an evolving emergency scenario that your group colleagues will be tasked to provide answers. In this session, the initial scenario will be introduced along with the instructions for how to address the scenario.

1500 **Day Concludes**

Tuesday, April 14, 2026

0830 – 0900 **Tea/Coffee**

0900 - 1030 **Session 03: Autonomy, AI, and Its Evolution 1**
Moderator: ***Fahad Malaikah****, Professor of Practice, NESA Center for Strategic Studies*
Speakers:
- ***Mr. Martijn Rasser****, Senior Director for Economy, Special Competitive Studies Project*

1030 – 1100 **Break**

1100 – 1200 **Session 04: Strategic and Technological Competition**
Moderator: ***Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speakers:
- ***Ms. Lisa Curtis****, Senior Fellow and Director, Indo-Pacific Security Program, CNAS*

1200 – 1300 **Lunch**

1300 – 1415 **Session 05: Autonomy, AI, and Its Evolution 2**
Moderator: ***Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speakers:
- ***Ms. Schuyler Moore****, VP Innovation at Saab UK and Managing Director at BlueBear (VIRTUAL)*

1415 – 1445 **Media Alumni and Global Net Briefs**
- ***Mr. Christopher Muller,*** *Program Manager, Outreach & Engagement, NESA Center for Strategic Studies*

1445 **Day Concludes**

Wednesday, April 15, 2026

0830 – 0900 **Tea/Coffee**

0900 – 1045 **Session 06: Tech, Air, and Aerospace**
Moderator: ***Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speakers:
- ***Mr. Clayton Swope****, Deputy Director, Aerospace Security Project and Senior Fellow, Defense and Security Department, CSIS*
- ***Dr. Kelly A. Grieco****, Senior Fellow, Reimagining US Grand Strategy Program, Stimson Center*

1045 – 1115 **Break**

1115 – 1230 **Tabletop Exercise Session 1**

1230 – 1345 **Lunch**

1345 – 1515 Tabletop Exercise Session 2

1515 Day Concludes

Thursday, April 16, 2026

0830 – 0900 Tea/Coffee

0900 – 1045 Session 07: Cybersecurity and National Security
Moderator: ***Fahad Malaikah****, Professor of Practice, NESA Center for Strategic Studies*
Speakers:

- ***PART A***
  Dr. Paul Lyons*, Principal Deputy Assistant Secretary of War for Cyber Policy and performing the duties of Deputy Assistant Secretary of War for Cyber Policy, U.S. Department of War*

- ***Part B***
  Dr. Jim Chen*, Professor, Cyber-enabled National Security Strategies, Artificial Intelligence, Cyber Operations, College of Information and Cyberspace, National Defense University*

1045 – 1100 Break

1100 – 1230 Tabletop Exercise Session 3

1230 – 1330 Lunch

1330 – 1500 Session 08: Public-Private Partnerships, Incubation, and Dual-Use
Moderator: ***Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speakers:

- ***Dr. Gwyneth Sutherlin****, Director of UC2- the University Consortium for Cybersecurity for the Department of Defense, National Defense University*

1500 – 1515 Break

1515 – 1615 Session 09: Cybersecurity and Cyber Deterrence
Moderator: ***Fahad Malaikah****, Professor of Practice, NESA Center for Strategic Studies*
Speaker:

- ***Dr. Chris C. Demchak****, Professor, Cyber and Innovation Policy Institute, Naval War College (VIRTUAL)*

1615 Day Concludes

Friday, April 17, 2026

0900 – 1100 Session 10: Current U.S. Policy Approaches
Moderator: ***Fahad Malaikah****, Professor of Practice, NESA Center for Strategic Studies*
Speakers:
- ***Dr. Hassan Abbas****, Distinguished Professor of International Relations, NESA Center for Strategic Studies*
- ***Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
- ***LTG (ret) Terry Wolff****, Distinguished Professor, NESA Center for Strategic Studies*

1100 – 1115 Break

1115 – 1200 Tabletop Exercise Presentations and Discussion
- Group 1 Presentation
- Group 2 Presentation

1200 – 1245 Director's Remarks and Certificate Ceremony
Announcer:
- ***Mr. Frejus Bakpe****, Course Operations Manager, NESA Center for Strategic Studies*

Presenter:
- ***Ambassador John Desrocher****, Director, NESA Center for Strategic Studies*

1245 – 1300 Farewell Remarks
Speaker:
- ***Jeff Payne,*** *Assistant Professor, NESA Center for Strategic Studies*

1300 – 1345 Farewell Reception
Location: Lincoln Hall, 3rd Floor Hallway (Flag Hall)

1345 Course Concludes

TABLETOP EXERCISE SCENARIO:

The following scenario is built upon real world examples of the complexities associated with adapting to a world increasingly defined by technological innovation and its impact upon the security realm.

INITIAL INSTRUCTIONS:

Each of you is assigned to one of two exercise groups. Each group will have one of the two program leaders in the room to assist you. Group 1 has Professor Payne attached to it. Group 2 has Professor Malaikah attached to it.

Your first task in your respective group is to determine a process for the following responsibilities:

- Designate a Presenter or Presenters for your group's final conclusions at the end of the week.
- Designate a format for notetaking and slide deck creation with NESA's interns assigned to your respective group to track your deliberations and to facilitate the final presentation your group will make at the end of the week.
- NOTE: all members of the group are expected to assist the notetakers and presenter in the fulfillment of their responsibilities

After these roles are determined, your group will begin the formal exercise.

The exercise occurs in stages with additional data being revealed over time. During the exercise, the two groups should not interact with one another.

GROUP 1 – SPECIFIC INSTRUCTIONS

- Group 1, during the exercise, cannot communicate with any member of Group 2.
- Group 1 is not permitted to use any data, tool, or technological device during the exercise. This includes your personal phones, laptops, or other digital devices.
- Any clarification needed regarding the exercise or additional questions requiring an answer can be directed to the program leader (Professor Payne).

GROUP 2 – SPECIFIC INSTRUCTIONS

- Group 2, during the exercise, cannot communicate with any member of Group 1.
- Group 2 is permitted to use any data, tool, or technological device during the exercise. This includes your personal phones, laptops, or other digital devices. In fact, you are encouraged to use data from outside sources.

- Any clarification needed regarding the exercise or additional questions requiring an answer can be directed to the program leader (Professor Malaikah).

CRISIS SCENARIO: SKYNET'S SKIRMISH

Each group represents the principles of the national security council of the United States during this crisis. You are charged with determining the nature of the threats present, the source of the threats to the United States, a recommended course of action in responding, and initiating mitigation or counters to similar threats in the future.

- You will use the United States' structure, national power, economic aspects, and global influence for inspiration in your responses to the crisis but note that this is a hypothetical threat – it is inspired by real world examples, but not a replication of any actual past threat.

- For this exercise the principles of the national security council include the following institutions/roles: Secretary of State, Secretary of War, Secretary of Energy, Secretary of Homeland Security, Secretary of the Treasury, National Security Advisor, Chairman of the Joint Chiefs of Staff, and Director of National Intelligence
    - Additional institutions/roles that can be included as needed

- Your job is to navigate the crisis and provide recommended actions to the President.

DAY 1: THE CRISIS BEGINS

The White House Chief of Staff calls together the NSC to determine the response to a variety of cyber threats that have emerged in the past 5 hours.

- Over 15 power utility firms have reported anomalous network strains. These include power networks in both rural and urban environments, and the strains are not concentrated in any particular region of the country. Thus far, the three main power grid networks within the U.S. are functional.

- A major cloud computing provider has informed the U.S. government that large lateral movements among clients is occurring. This is unusual activity based upon the number of clients involved, the size of the data being transferred, and the lack of large events that would warrant such activity.

- Finally, social media outlets, particularly Instagram and X/Twitter, have seen a spike in announcements of an incoming massive cyber attack in the United States. The accounts making these claims are being taken seriously be private sector leaders, media outlets, and tech social media influencers.

Key Decisions:

- Determine if this is a national security threat/emergency.
- What actors/institutions need to be consulted in navigating this scenario?
- Should the threat be acknowledged publicly? If so, then how?
- Should national threat levels be raised – cyber, military, homeland security?

DAY 2: ESCALATION

Early indications of a major national cybersecurity crisis proved correct. Approximately 16 hours after your initial determinations, the country is now facing a real crisis.

- Major interruptions to financial payment systems are occurring – these interruptions are affecting normal household bill payment, major financial transfers among banks, and stock/bond trading. Private sector leaders are demanding trading be halted.

- Rolling blackouts have hit five areas – the Philadelphia metropolitan area, the San Francisco Bay area, northern Iowa (rural area), the El Paso metropolitan area, and much of West Virginia (rural area).

- Hospitals across multiple states have lost access to critical systems that govern operations, manage patient data, and regulate communications with emergency services/government institutions/other hospitals.

- A horde of government emails are illegally posted online, many of which are from the Department of Homeland Security.

Key Decisions:

- Do you publicly attribute the attacks against the suspected actor or wait for certainty?
- What problems in this crisis should be prioritized through the allocation of resources, personnel, and other government assets?
- Should national emergency authorities be declared/implemented?
- Do you authorize a response against the perpetrators? What sort of response?

DAY 3: PLATEAU

Despite the crisis persisting to a third day, core services have proven resilient. Emergency services have adapted to interruptions, hospitals have managed the crisis by returning to analog means, and power has largely been restored to all impacted areas. Public fear remains high, particularly regarding the financial impact of the crisis. There are new factors to consider.

- Similar "problem sets" have appeared among several U.S. allies and partners. Most are concentrated in Europe, but they have also emerged in Latin America and East Asia.

- The U.S. Coast Guard has confirmed foreign partner reports of substantial activity by known "black fleet" vessels. Some seemingly are loitering near undersea cables. Others seem to be on their way to ports inside states that are currently under international sanctions. Finally, more than a dozen known "black fleet" vessels are running dark in the Caribbean Sea and appear to be conducting a ship-to-ship transfer with other vessels running dark.

Key Decisions:

- Do you alter the priorities of the government?
- How do you calm the fears of the public?
- Does the government need to change its response to the suspected perpetrators?
- What policy alterations, improvements, and preparations need to be implemented based on this scenario?

NOTE: Upon completing your deliberations, please summarize your discussions over the three sessions into a slide deck that can be presented before the entire plenary.

INJECTS by NESA Faculty:

Day 1:

- Conflicting reporting that criminal ransomware groups are claiming responsibility for the cyber disruptions.
- Media outlets are emphasizing a report published a month prior detailing how much of the software relied upon for core infrastructural processes is not secure. The supply-chain in the development of the software includes inputs from companies located in countries hostile to U.S. interests.

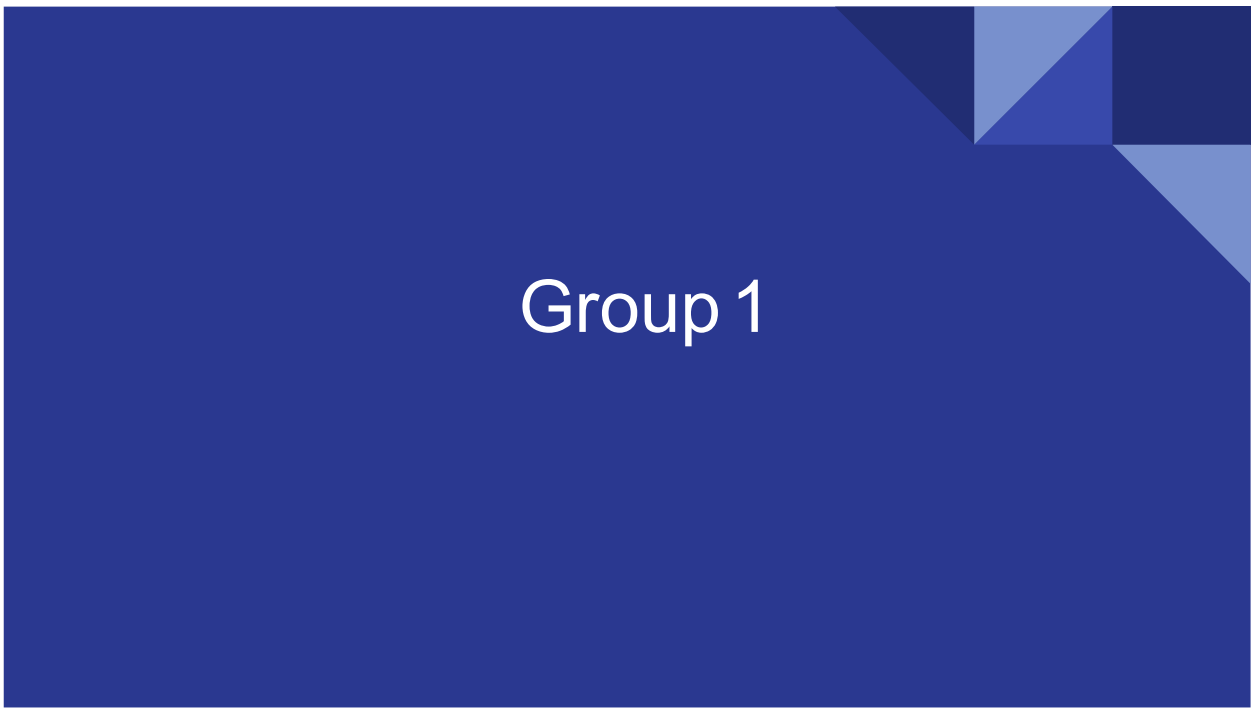
Day 2:

- Interruptions to U.S. military logistical systems are being relayed to the NSC, but there is no evidence yet that this is related to the larger crisis.
- The Media begins to call the crisis the "Cyber Pearl Harbor."
- Despite many "hacking groups" claiming responsibility, U.S. investigations have determined that a group called T800 (reference to the terminator in the original film) that runs various black market digital tools for various cartels, including arms traffickers, narcotraffickers, and violent extremists is responsible for the attacks.

Day 3:

- KEY DATA POINT 1 – T800's members are not concentrated in any state, but to have the success it did it either had to hack firms inside states hostile to the U.S. or have support by those states to exploit the software.
- KEY DATA POINT 2 – the investigation reveal that some of T800's partners/clients are drug cartels who used the crisis to exploit the border for trafficking and to launder money more easily out of the U.S.

TABLETOP EXERCISE RESULTS/SLIDES:

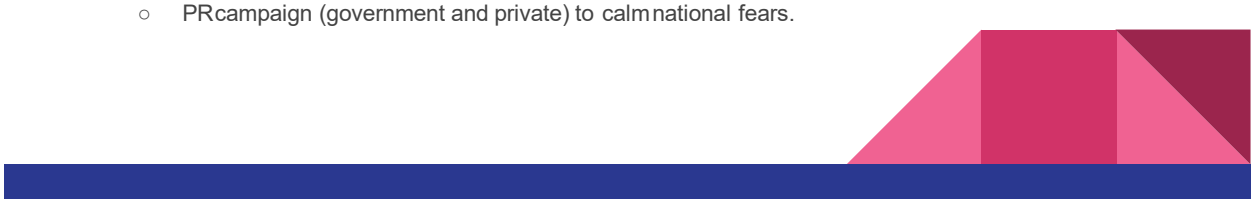


Day 1:

- Indicators
  - Visible widespread problems with the U.S. energy grid.
  - Strange occurrences within the cloud.
  - Widespread speculation on social media of a cyber attacks against the USA.
- Recommendations/Response
  - Assessed as a threat
  - Assigned DoE DHS, HHS, DoJ, DoS, IC, and DoC
  - Risk assessment and escalation mapped (Updated as necessary).
  - Acknowledgment and Statement from the White House

Day 2:

- Indicators
  - Major financial interruptions.
  - Rolling Blackouts.
  - Hospital systems failing.
  - DHS hacked/Data leak.
- Recommendations/Response
  - Recommended declaration of emergency.
  - Linked actions
    - Identified cyber threat actor.
    - Intensified collaboration among DoE DHS, HHS, DoJ, DoS, IC, and DoC
    - Implement comprehensive countermeasures in regards to cyber threats.
  - Risk assessment and escalation mapped (Updated as necessary).
  - PR campaign (government and private) to calm national fears.



Day 3:

- Indicators
  - Resilience proven-core U.S. services.
  - Global escalation.
  - Maritime threat presents-Black Fleet.
  - Massive narco operation occurred.
- Recommendations/Response
  - Escalation from cyber to multi domain/cross domain
  - International coordination/cooperation
  - Risk assessment and escalation mapped (Updated as necessary).
  - PR campaign (government and private) to overcome financial fears.
  - Tasker of compiling lessons learned/ after action report.
  - Compile options for operations against threat actors

ARAB/ENG breakout room Situation Slides

Near East South Asia (NESA) Center for Strategic Studies
May 2026

Day 1:Threat Assessment & Response Strategy

Situation viewed as a **national security threat** with potential to escalate into an emergency

Not yet a crisis — systems largely remain functional

- **Cyber Threat Level:** 4 → 3
  - Maintain flexibility to raise to Level 2 if conditions worsen
- **Military Threat Level:** No change (remain at Level 4)
  - No direct impact on military operations at this time
- **Homeland Security Level:** 4 → 3
  - Ensures consistency with broader threat posture

Key Partners & Coordination Strategy

Gov Actors

- NSA (ISR): intel & attribution
- Cyber Command: response
- DHS/CISA: industry coordination
- DOE: infrastructure
- FBI: forensics

Leadership

- NSC/White House: central coordination

External Partners

- Telecom & Big Tech: infrastructure
- ISACs: info sharing
- CERT/CISA + cyber firms: diagnosis & attribution

Day 2:

Priorities

- Identify breach + attack type
- Share intel in real time

Public Comms

- Confirm before blame
- Be transparent, limit misinformation

Beyond Gov

- Private sector collaboration
- Zero Trust adoption
- Stronger cyber standards
- Network backups & resilience

Day 2

Prioritization:

1. Power and infrastructure
2. Water/health systems
3. Information
4. Financial

Immediate Focus

- Mitigate damage first
- Attribute/blame later

Public Messaging

- Reassure population
- Avoid naming actor (maintain flexibility)

Policy Action

- Declare national emergency

Day 3: Evolving Priorities: From Recovery to Offense

1. Energize all parties/institutions to direct their attention against perpetrators.

- Military presence-->Deterrence via aggression
- Joint naval response
- NATO/ ally support for protection of undersea cables is possible due to provisions contained in UNCLOS

2. Revive stability of financial services; bank protective services, offensive strategy

3. Reassess existing policies, SOP in place for future cyber crises (promote efficient coordination)

Attribution and Containment

- Coordinated response across all levels of gov't to give daily updates on act. Public attribution (name aggressor)

  <u>3 levels</u>

1. Joint level (states)
2. National level; coordinated press sec briefing that included multitude of players at varying times.
3. Institutional level ie industry, military etc…what actions are being taken

- Digital activity and purposeful messaging
- Contingency plan in event that communications are compromised