NESA Executive Seminar: Technology and Security
Report/Executive Summary
August 2022

Executive Summary:

From 25 July to 5 August, the Near East South Asia (NESA) Center for Strategic Studies conducted an Executive Seminar that focused on how the security sector is informed by technological advances. The event's topics including Autonomous/Unmanned Systems, Space, Cybersecurity, Artificial Intelligence, Information, and Digital Infrastructure, among others. Special sessions on energy, the Indo Pacific, and Women, Peace, and Security were also included in the program. Participants hailed from 23 countries from throughout Africa and Asia. The participants represented military institutions, diplomatic offices, law enforcement divisions, and other government elements from their respective countries. The event was led by Jeff Payne, NESA Assistant Professor, with facilitation/presentations provided by NESA faculty Dr. Roger Kangas, Dr. Gawdat Bahgat, Dr. Michael Sharnoff, and Professor David Des Roches.

The forum was a hybrid event to facilitate participants who could not attend in person. In-person activities took place at Fort Lesley J. McNair at NESA's offices. The event featured speakers from various elements of the United States Government, including NESA faculty, DKI APCSS faculty, ACSS faculty, the Office of the Secretary of Defense for Policy, the Defense Innovation Unit, and NAVCENT. Themes from the participants are detailed below and are accompanied by the agenda of the event, results of participant surveys, and responses from breakout sessions.

THEMES:

The following themes and/or questions were routinely mentioned among speakers and participants during the event.

- Trust emerged as a theme of the seminar. Building trust among nations is difficult in and of itself, but when adding in the sensitive nature of certain technological elements and the hurdles become higher for trust building. How do nations gain trust in technology? How do nations share/transfer technology? These questions came up throughout and were discussed by participants.

- How do more technologically advanced nations provide assistance in technological terms with developing states? Is the best format premised on private enterprise sales, or should they be managed in government-to-government relationships? Many developing states

need technological tools that are already integrated into the operations of developed states and gaining access to those tools is a stated objective of many regional states.

- Information sharing is making advances through technology as it lowers the logistical bar, but there are new challenges that emerge because technology, specifically networks and information technology, are sensitive in nature. Namely, who hosts the information that is shared and how do states determine the line between information that should be shared with partnering states and information that is too sensitive to be shared at all?

- The cost of adopting and integrating recent technology is prohibitive in most cases. How can partnering nations lower the cost for actors to gain access to necessary technology?

- How can states better integrate technology that has both a public and private usage? Many of the advancements in satellite technology and algorithmic data management are coming from the private sector and are designed for a commercial use. Governments and their security organizations are not traditional consumers for technology. Is it a problem for countries to adapt technology that is commercially available? To put the quandary in another way – how do security services deal with the fact that many key technologies are already commercial?

- The revolution in space was a theme that garnered a lot of attention by participants. What is being developed for orbit and how that technology is being used were just a few of the questions that were asked.

- Trend lines with technology introduce a question of the mechanics by which states cooperate with one another on information sharing and technology transfer. Should it be done bilaterally, multilaterally, or through an international organization? Does a common mechanism matter, or is it simply dependent upon the preferred method by a state? These questions came up routinely during breakouts and plenary sessions.

- Industrial policy came up in discussions as well, specifically in relation to technology development and improvement. How will states prioritizing certain technologies impact the private sector – are states capable of improving technology policy or will they diminish research and development? Does the idea of states sponsoring technology and even picking winners/losers in technological development in their own territories mean greater chances of cooperation or more competition?

- Communication during the digital age came up routinely as well during the seminar. Do states keep up with non-state actors in communicating not only about technology, but security in general? Are illicit actors better at exploiting modern communications than the state due to the state's overreliance on traditional media formats and slower pace of communication?

- Finally, a theme that emerged near the end of the seminar was the technology surrounding climate change. NESA states face challenges from climate and developing technologies offer some ways to mitigate the impact of these changes. How can states work on climate? Will it be ad hoc or part of a system of some sort? What technologies will be key to address climate change?

WORKSHOP RECORD:

Monday, 25 July

All discussions will be held off-the-record, under Chatham House rules of non-attribution. All Participants are urged to contribute to the discussion in all sessions. Digital participants possess two ways of communicating – by using the text function to write their questions or to raise their hand to inquire. In-person participants can raise signal from their seated position that they have a question. All question-and-answer sessions will move back and forth between digital and in-person questions.

0800-0930 **Registration** (for In-Person Participants)

0930-0945 **Course Director's Welcome**
Speaker: ***Mr. Jeff Payne,*** *Assistant Professor, NESA Center for Strategic Studies*

0945-1000 **Academic Dean's Welcome**
Speaker: ***Dr. Roger Kangas,*** *Academic Dean, NESA Center for Strategic Studies*

1000-1015 Break

1015-1100 **Welcome Session**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center Speaker:* ***Professor Tom Wingfield****, Senior International and Defense Research, RAND Corporation*

1100-1115 **Alumni and Media & Communications Brief**
Speaker: ***Gillian Hurtt****, Education Technology Specialist, NESA Center for Strategic Studies*

1115-1215 **Session 01: Translating Technological Applications**
This introductory session addresses how policymakers translate technological platforms into governance.
Moderator: ***Dr. Gawdat Bahgat****, Professor, NESA Center for Strategic Studies*
Speaker:
Ms. Emelia Probasco, *Senior Fellow, Georgetown's Center for Security and Emerging Technology (CSET)*

1215-1230 Break

1230-1400 **Women, Peace, and Security Roundtable (Plenary and Digital Participants)**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center and* ***Professor Anne Moisan****, Associate Professor, NESA Center for Strategic Studies* Speaker: ***Dr. Michael E. Brown****, Professor of International Affairs and Political Science, Elliott School of International Affairs*

1400 Day concludes

Tuesday, 26 July

0730-0800 **Online Check in, Coffee Networking Session**

0800-0915 **Session 02: A Debate – Open versus Closed Systems**
Moderator: ***Dr. Michael Sharnoff****, Associate Professor, NESA Center for Strategic Studies* Speaker**:**
Mr. Agam Rafaeli-Farhadian*, Executive Board Member, the Public Knowledge (Digital)*

0915-0945 Break; Group Photograph on the Steps of Marshall Hall, National Defense University

0945-1115 **Session 03: Great Power Competition and Technology**
Moderator: ***Dr. Gawdat Bahgat****, Professor, NESA Center for Strategic Studies*
Speakers:
Ms. Hannah Kelley*, Research Assistant, Technology and National Security Program, Center for a New American Security*
Dr. Andreas Kuehn*, Senior Fellow, Observer Research Foundation America (Digital)*

1115 Day concludes for Digital Participants

1115-1215 Lunch (In-Person Attendees); GlobalNet Briefing and Tutorial During Lunch

1215-1330 **Discussion Session 1: The Challenge of Too Much Information**

- In this initial breakout session, the in-person plenary will be broken down into smaller groups. Each group will face the challenge of making strategic and operational choices based upon a developing national security emergency. Their main task is to determine what information is relevant and reliable and what information is unnecessary/unreliable.

1330 Day Concludes

<u>Wednesday, 27 July</u>

0730-0800 **Online Check in, Coffee Networking Session**

0800-0945 **Session 04: Defining and Measuring the Cyber/Technology Challenge**
Moderator: ***Dr. Gawdat Bahgat****, Professor, NESA Center for Strategic Studies*
Speakers:
Dr. Gwyneth Sutherlin*, Assistant Professor, College of Information and Cyberspace, National Defense University*
Dr. Nathaniel Allen*, Assistant Professor for Security Studies, Africa Center for Strategic Studies*

0945-1000 Break

1000-1145 **Session 05: Asymmetry and Technology**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies* Speakers:
Mr. Gregory B. Poling*, Senior Fellow for Southeast Asia and Director, Asia*

Maritime Transparency Initiative, CSIS
***Capt. Michael D. Brasseur**, Commander, Task Force 59, U.S. NAVCENT (Digital – TBC)*

1145-1150 Day concludes for In-Person Participants; Break for Digital Participants

1150-1230 **Digital Activity 1 – Short Response Activity and Trust in Technology Assessment (led by Mr. Payne)**

- This activity, designed for digital participants only, will examine what technological platforms are commonly used and of those, which are commonly trusted. From this initial line of inquiry, the participants will explain their logic for their decisions.

1230 Day Concludes

Thursday, 28 July

0730-0800 **Online Check in, Coffee Networking Session**

0800-0945 **Session 06: Perspectives from Space**
Moderator: ***Dr. Gawdat Bahgat**, Professor, NESA Center for Strategic Studies*
Speakers:
***Ms. Kaitlyn Johnson**, Deputy Director and Fellow, Aerospace Security Project, CSIS*
***Ms. Grace Kim**, Space Policy Advisor, Office of the Secretary of Defense (Policy)*
***Mr. Dave Zikusoka**, Special Assistant to the United States Secretary of Defense*

0945-1000 Break

1000-1145 **Session 07: Drones, Unmanned Systems, Autonomous Vehicles**
Moderator: ***Dr. Michael Sharnoff**, Associate Professor, NESA Center for Strategic Studies* Speakers:
***Pr. David Des Roches**, Associate Professor, NESA Center for Strategic Studies*
***Mr. Ryan Fedasiuk**, Research Analyst, Center for Security and Emerging Technology, Georgetown University*

1145 Day concludes

Friday, 29 July

NOTE: ALL DIGITAL ATTENDEES ARE EXEMPTED FROM TAKING PART

0930 Participants Board Bus for Excursion

0930-1000 Transport to Arlington National Cemetery

1000-1130 **Tour of Arlington National Cemetery**

1130-1200 Transport to Luncheon Location

1200-1330 Lunch at Ambar Restaurant

1330-1400 Return to Hotel

1400 Arrive at Hotel

Monday, 1 August

0730-0800 **Online Check in, Coffee Networking Session**

0800-0900 **Session 08: Intention and Trends in U/A Vehicles**
Moderator: ***Dr. Michael Sharnoff****, Associate Professor, NESA Center for Strategic Studies* Speaker:
Dr. Sarah Kreps*, John L. Wetherill Professor, Department of Government, and the Director of the Cornell Tech Policy Lab, Cornell University (Digital)*

0900-0930 **Special Session: Indo Pacific and Data Experimentation**
Speaker: ***Mr. Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*

0930-1000 Break

1000-1145 **Session 09: Maritime Domain Awareness and Technology**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies* Speakers:
Mr. Gunther Errhalt*, Global Patrol Support Office, Global Fishing Watch (Digital)*
Mr. Jay Benson*, Director, Stable Seas (Digital)*

1145-1150 Day concludes for In-Person Participants; Break for Digital Participants

1150-1230 **Digital Activity 2 – Short Response Activity and Plugging Gaps in Knowledge (led by Mr. Payne)**

- Digital participants will start this effort by facing a particular scenario – you represent a country that always has its digital infrastructure under assault in an escalating manner. You need solutions now to ease the burden and that means you need a digital workforce capable of addressing the technical problem sets while still being able to work within the structures of your government. How do you fill this gap in the immediate term?

1230 Day Concludes

Tuesday, 2 August

0730-0800 **Online Check in, Coffee Networking Session**

0800-0930 **Session 10: Digital Infrastructure and Security**
Moderator: ***Dr. Gawdat Bahgat****, Professor, NESA Center for Strategic Studies*
Speaker:

Dr. John Hemmings, *Professor, Daniel K. Inouye Asia-Pacific Center for Security Studies (Digital)*

0930-1000 Break

1000-1130 **Session 11: Are the bad guys ahead? Illicit Actors and the Use of Technology**
Moderator: ***Dr. Michael Sharnoff****, Associate Professor, NESA Center for Strategic Studies* Speakers:
Ms. Maisie Pigeon*, Independent Maritime Security and Transnational Crime Consultant (Digital)*
Dr. Catherine Lena Kelly*, Associate Professor of Justice and the Rule of Law, Africa Center for Strategic Studies*

1130 Day concludes

<u>Wednesday, 3 August</u>

0730-0800 **Online Check in, Coffee Networking Session**

0800-0930 **Session 12: Information Challenges**
Moderator: ***Dr. Michael Sharnoff****, Associate Professor, NESA Center for Strategic Studies* Speaker**:**
Dr. Roger Kangas, *Academic Dean, NESA Center for Strategic Studies*

0930-1000 Break

1000-1130 **Session 13: The Idea of the Public/Private Partnership**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speaker:
Dr. Jared Dunnmon*, Technical Director - Artificial Intelligence/Machine Learning, Defense Innovation Unit (DIU) (Digital)*

1145 Day concludes for Digital Participants

1145-1245 Lunch (In-Person Attendees)

1245-1400 **Discussion Session 2: Cyber Crisis – Non-State Actor Hostility**

- The plenary will once again be broken down into smaller groups and face a theoretical challenge that is all too relevant to our world. They will each respectively represent a nation that is a net importer of foodstuffs (necessary to feed the population) and fuel (to run the economy). This hypothetical nation relies heavily on its ports and that port information systems, from manifests, customs data, to balance surplus stores, has been potentially hacked. The hackers are using a ransomware method. You face a crisis. What do you advise?

1400 Day Concludes

Thursday, 4 August

0730-0800 **Online Check in, Coffee Networking Session**

0800-0900 **Energy and Technology**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies* Speaker:
Dr. Gawdat Bahgat, *Professor, NESA Center for Strategic Studies*

0900-0930 Break

0930-1100 **Session 14: Did Covid Change Perceptions of Tech**
Moderator: ***Dr. Michael Sharnoff****, Associate Professor, NESA Center for Strategic Studies* Speaker**:**
Dr. Jaclyn A. Kerr*, Senior Research Fellow, Defense and Technology Futures, Institute for National Strategic Studies (INSS), National Defense University (Digital)*

1100 Day concludes for Digital Participants

1100-1200 Lunch (In-Person Attendees)

1200-1315 **Discussion Session 3: Cooperative Planning**

- The final breakout session will task the participants with developing a methodology by which information pertaining to common security challenges can be shared. Data sharing, seen as critical in our day, remains irregular and insufficient. Your task is to devise a means to overcome that deficiency.

1315 Day Concludes

Friday, 5 August

0730-0800 **Online Check in, Coffee Networking Session**

0800-0930 **Session 15: State Responsibility in the Digital Age (a Roundtable of Observations)**
Moderator: ***Mr. Jeff Payne****, Assistant Professor, NESA Center for Strategic Studies*
Speakers:
Dr. Michael Sharnoff*, Associate Professor, NESA Center for Strategic Studies*
Dr. Gawdat Bahgat*, Professor, NESA Center for Strategic Studies*

0930-1000 Break

1000-1015 **Academic Dean's Farewell**
Speaker: ***Dr. Roger Kangas****, Academic Dean, NESA Center for Strategic Studies*

1015-1030 **Deputy Director's Farewell**

Speaker: ***COL David Lamm, USA (Ret.),*** *Deputy Director, NESA Center for Strategic Studies*

1030-1100 **Course Director's Farewell**
Speaker: ***Mr. Jeff Payne,*** *Assistant Professor, NESA Center for Strategic Studies*

1100 Seminar concludes

1100-1145 Farewell Reception for In-Person Participants

BREAKOUT RESULTS:

PLEASE NOTE THAT NOT ALL RESPONSES FROM EACH PARTICIPANT ARE REFLECTGED IN THIS RECORD – THERE WAS TOO MUCH DATA TO COMPILE IT ALL IN A COHESIVE MANNER. NESA SEEKED TO MERGE AS MUCH DATA TOGETHER AS POSSIBLE.

BREAKOUT 1 (IN PERSON)

The Challenge of Too Much Information:

In this breakout session the plenary will be divided into three smaller groups. Each group will address the same scenario. Your first task is to review the national security threat presented to you in detail. From that point, each group should determine what pieces of information pose the greatest threat and from there develop an effective response.

Each group should elect a note taker who will compile the conclusions of the group and either share a hard copy or send a digital copy to the NESA faculty team.

The Scenario:

A small, but very destabilizing violent extremist organization has emerged. Its aim is to do all that in can to undermine the stability of your country. The organization is political, not cultural, ethnic, or religious in nature. It exploits a rural area within your country that includes the border zone with your northern neighbor. This area of the country is less prosperous than the rest of the

country. The country's military and national law enforcement institutions are engaged in operations meant to weaken the ability of this violent extremist organization to cause damage.

Yet, the violent extremist organization is very effective at spreading misinformation, especially through social and digital media platforms. You are each a member of a group of experts brought together by your country's government to develop a response to the misinformation that this group spreads. This misinformation is undermining the efforts of the military and law enforcement to counter their violence, creating suspicion in the international community about your country's response to the organization, and causing friction with your immediate neighbors.

The misinformation that you must counter is the following:

- The violent extremist organization has created a free-to-use mobile game that appeals to children and adolescents. The game routinely promotes the ideology of the violent extremists. The game can be downloaded from any phone's application store and was created and uploaded outside your country.

- The violent extremists rely on the cellular networks of your northern neighbor, so their phones are not connected to your own infrastructure.

- They routinely use major social media websites to create profiles that highlight local music, social media trends, and short videos designed to be funny, and intermix them with highly edited videos of the military/law enforcement operations meant to gain sympathy.
- They maintain strong social media presence in other languages in profiles targeting foreign audiences to create the perception that they are being innocently targeted.

- As the area is rural and there is violence, national media outlets that cover stories often rely on law enforcement to ensure security. The violent extremists use members to shoot videos of the media arriving with law enforcement to create the perception of bias by the media.

- They routinely shoot videos talking about how great society is in neighboring states and compare that to scenes of violence they created in your country.

- Several members routinely use conspiracy-oriented subgroups in social media to imply that their organization does not actual exist and the government is merely using violence against people living in the rural area. These members never appear in other parts of the group's social media presence to maintain the appearance of not being affiliated

- The organization closely follows government social media feeds and other media forums to monitor government activities – in essence, they use the transparency of the government to hide themselves from authorities.

- Local assistance against the organization is minimal, as local communities perceive that the organization will target them if they help the government.

- The rest of the country routinely shares rumors about the group that portray the extremist group as being larger and more powerful than they are.

- Communication experts in your country argue that government responses in media do not keep pace with the extremist organization's messaging.

- Through media reports that extremists in turn promote, the public has become aware of a debate within the government as to how to best handle communications regarding countering this violent extremist organization. Some government officials recommend censoring media reports on the group, while others are arguing for a more transparent approach to public reporting.

What is your approach to this misinformation?

RESPONSES:

The responses from each of the three breakout groups were varied and brought up for discussion the lessons they have learned from their own experiences in their home countries. In no particular order, these are some of the common responses that emerged from the groups.

- What is the nature of relations with the neighboring state that the violent extremist group relies upon for their communications. Is this a case of a porous border region between friendly states that these extremists have recognized and used to their advantage? Are relations not deep or even potentially hostile? Is the problem the neighboring state or the nature of modern cellular and communications networks? How aware or even responsible is the neighboring state?

- What can the hypothetical country the participants represent do to minimize the digital presence of the extremist group? Some argued to propose a temporary shutting down of any telecommunications system to stop the messaging. Some proposed working with neighboring states to put pressure on technology firms whose platforms the extremist groups use. Others proposed a more offensive method where the nation's own technological-skilled workers use the same system to track and better understand how the extremist group uses the digital realm. Still others proposed stronger regulations and legal systems that govern social media, telecommunications, and other digital platforms.

- All groups discussed in length how the state should communicate regarding this scenario. As the extremist group targets youth, the state should make specific messages focused on parents and households to use societal ties to counter extremist messaging. Others recommended intensifying outreach to the region of the country most impacted by the extremists to show how the state is responding to the violence. More recommended that the state moves with all speed to gather as much information on the extremist group as possible and devise better counter communications based on that effort, including using the group's own methodology against them. There were discussions on what role the media plays in this scenario – should reporters have access to the area of violence? If they have access, then are there elements that should not be reported due to national security concerns?

- All groups discussed that removing the violent extremist organization as a threat is a certain way to remove the misinformation. So long as the group is active, then it will always find ways to get out its misinformation. Work to progress the efforts of police and military forces to gain control of the region in question.

- The groups also discussed how this scenario brings up key diplomatic questions. There is a diplomatic element to the scenario – both in terms of public diplomacy and government-to-government diplomacy. It is a security threat, but that cannot and should not be addressed merely with security forces. Other elements of the government, including diplomatic corps, are key to alleviating public concern, getting out more accurate information to the international community, and helping to build a public sense of the aims of the government in this case. The diplomats of the country would also be essential for designing treaties to counter such threats in the future and working more closely with the neighboring state whose communications network is being used by extremists. Diplomats in most countries are also the government representatives who can navigate elements of human rights, communications, and government authority. Such a balance is more difficult for security forces because they have a different mission.

- All groups also put an emphasis on the region in which this extremist group is operating. It is operating in a less developed, border region between the country in question and its norther neighbor. Border regions are always transit zones, as they feature international trade. To what degree is this border region the real issue? The state should certainly aim to better develop it in the long-term and work to make sure that regional residents understand they live within the state and the state will integrate them more effectively in governance.

- All groups also discussed the degree by which this scenario represents a crisis. Is it a crisis for a specific part of the country or for the country as a whole? Is it a crisis that we can counter without altering the status quo, or do certain changes need to be made from restricting information about the conflict to limiting telecommunications access? Is this situation mainly a law enforcement concern or a military concern? All three groups discussed such questions in depth.

- Finally, each group made the point that any response must include multiple efforts simultaneously. Security forces need to continue their work and at the same time diplomatic efforts need to be undertaken, public communications need to be rolled out, and cybersecurity professionals need to undertake their investigations. This is a wholeof-government challenge.

BREAKOUT 2 (IN PERSON)

Cyber Crisis – Non-State Actor Hostility:

In this breakout session the plenary will be divided into three smaller groups. Each group will address the same scenario. Your first task is to review the national security threat presented to you in detail. From that point, each group should determine what pieces of information are most relevant and devise a policy recommendation. The objective is to respond with as much precision as you can with limited data.

Each group should elect a note taker who will compile the conclusions of the group and either share a hard copy or send a digital copy to the NESA faculty team.

The Scenario:

You represent an intergovernmental working group brought together to determine the accuracy of a ransomware threat. Three days ago, the national police service received a threat from an unknown actor that demanded a payment of 50 million U.S. dollars, or they will initiate a shutdown of all logistics systems tied to the primary ports of your country. Everything from the accounting of your imports and exports to the stability of your electrical grid and internet services could be impacted. The potential damage is in the billions of U.S. dollars. The actor claims to have already hacked the systems and merely must initiate the code already present to gain control. In the threat, the ransomware actor said that if payment was not sent in five days, then the code will automatically initiate.

Since the initial threat, different departments of the government have made widely divergent recommendations to the leadership of the country, as well as pointed to connections to other factors that they feel is relevant to this case. The comprehensive government response has been confused. Thus far the threat has not been made public.

Your country's leadership is worried that this threat has not only revealed vulnerabilities in your country, but that government structures may not be designed to devise a coherent response. The leader brought you together to do one thing – determine what information is most dependable and recommend a course of action to address the ransomware attack.

The information you must judge is the following:

- The country's cybersecurity institutions were not able to determine the source or the identity of the ransomware attacker.

- The country's cybersecurity institutions were not able to determine if the software within the port systems is compromised.

- The commercial firm that designed the security software used to protect the port proclaimed that any hack would create glitches that could be traced, and this threat is likely a ruse.

- The former cybersecurity chief of the country approved the design of the port's cyber systems. He chose the design he did because it would not be centralized. Advice he received argued that such a system would be easier to hack but it would be highly unlikely for any hack to compromise the entire system.

- Your country's chief cybersecurity officer stated months ago that the port cyber infrastructure is made up of multiple software systems and therefore inherently vulnerable.

- The military highlighted that your country's chief international opponent made claims recently that they have developed new means by which to weaken their enemies. The military believes this attack is tied to that foreign country.

- The foreign affairs division of the government believes the attacker is a non-state actor or a disgruntled government employee with access since the threat was sent to the national police and not another government department.

- Nearly a year ago, the port authority partnered with a local university for a game where computer science students would attempt to hack a system like the one used by the port. The aim was to show vulnerabilities to the system. Of the 50 students, 2 students hacked the software. No changes were made to the port's infrastructure.

- The national police leadership wish to start investigating every port employee with access to the system, as well as encouraging the government to make the threat public to assist with leads.

- The port authority director has stated that the threat is potentially too severe, and the payment must be made to maintain commercial flow. Afterwards, the system can be changed or enhanced.

- The leader's chief security advisor believes the security cost of this threat is too high and recommends that the port be shut down immediately to diagnose the system's vulnerabilities.

Based upon the above, what do you recommend?

<u>RESPONSES:</u>

Responses from the three breakout groups featured these common traits.

- All three groups debated timing when it came to the ransomware threat. For some, the recommendation was to immediately prepare a response and pay no mind to the five days the ransom provided. Others wanted to use the five days to gather as much investigative data as possible before having to directly communicate with those behind the attack.

- Each group also discussed the validity of the ransomware attack. The fact that the ransom was delivered to the national police revealed that the origin of the attack was likely internal, as why would a foreign actor reach out to the police instead of national leaders or the diplomatic offices of the state? Each group brought up whether the ransomware attack was, in fact, real. Yet, all three groups agreed that the potential damages were too high to not take the ransom seriously.

- The scale of the attack was also discussed. Participants pointed out that a 50 million USD ransom was high but showed a lack of understanding of the scale of government functions. In busy ports, 50 million was a few days of trade. All ports have disaster protocols, including cyberattacks, that would allow them to transfer to backup systems or even transit completely to analog accounting. A cyberattack could disrupt, but not shut down a port. The real danger, for many, was that allowing such an cyberattack and not finding out the culprit would harm confidence in the government by the population and signal potential weaknesses to outside rivals/opponents.

- All three groups discussed how threats, such as ransomware attacks, are increasingly common and not all states have as deep of protocols as are necessary to increase the likelihood of stopping them or having a better chance of impeding such attackers. Cyber strategies need to be evolved, better interagency communication is key, better government accounting is essential to have a better understanding of what really is or is not happening inside systems, and so forth.

- The nature of threat was discussed in detail by all groups. The scenario provided information that initial investigations could not determine if the system was hacked or not. This was not sufficient for any participant. It may take longer than the five days to find out the format of the hack, but the time provided would at least give enough time for security specialists and software engineers to determine if any system attached to the port was accessed in an odd fashion or if new uploads/alterations to software had taken place.

- The unfortunate reality of payment was discussed by all three groups. All the groups recognized that the government, to some degree, must prepare for a backup plan of payment in the worse of cases. No one wants to pay, and all think it is a horrid idea in the long run, but the immediate danger must be overcome. Relatedly, the necessary officials must discuss if/how the port should be shut down. No one wants this option, but in the worst of cases, it may be necessary to purge the systems for a restart.

- The groups also had discussions on what could be called openness regarding this threat. Should the public be informed of the ransomware threat? Should ports really have interlinked systems that provide more avenues for non-certified personnel to access? These were all debates about how to design digital infrastructure and how to discuss such topics with the public.

- Each group also argued that such conversations need to be a feature of more international security discussions – key private firms can be consulted in such cases, specialized

response teams could be models for others to use, and so forth. Participants pointed out that how our respective systems work can remain security all the while sharing general best practices to diminish potential harm.

BREAKOUT 3 (IN PERSON)

Cooperative Planning:

In this breakout session the plenary will be divided into three smaller groups. Each group will address the same scenario. Your first task is to review the scenario presented to you in detail. From that point, each group should determine how to structure a response. The objective is to develop the most comprehensive and realistic information sharing structure possible.

Each group should elect a note taker who will compile the conclusions of the group and either share a hard copy or send a digital copy to the NESA faculty team.

The Scenario:

A group of states are making it a priority to intensify information sharing regarding cyberattacks. The aim of this effort is to reveal the source of the attack, the means of the attack, the impact of the attack, the response to the attack, and, finally, the improvements made after the attack. The objective is to create greater understanding of how cyberattacks occur and provide models for how states can better respond and improve their own security.

Your country is intending to join this effort and you represent the working group of government officials brought together to devise the national plan for information sharing.

There are many issues to consider. Cybersecurity systems are highly sensitive, so you need to consider how sharing data may undermine national security. You need to consider how you balance domestic politics and international trust building. The effort also requires you to think about the format through which the information will be shared – is it a central database, is it routine or sporadic, and who will host the information?

Comprehensively, you must determine what data you are willing to share and what means of communication are the most appropriate.

RESPONSES:

Responses from the three breakout groups featured these common traits.

- Trust was something discussed amongst all groups to one degree or another. There remains a lack of trust among nation-states within the NESA region and given the sensitive nature of cybersecurity for all states, it is difficult to initiate efforts meant to give up control over information that your own systems have acquired. All participants clearly see the value in cooperation and information sharing, but also understand the hurdles that exist to achieve that aim.

- Methodology for information sharing was also debated amongst groups. Participants rightfully pointed out that certain methods of international relations are more commonly

accepted within their own national system than others. Some states may be willing to share information with other states, but only in a bilateral format. Others would default to a multlateral formula. Still others would find it more productive for willing states to share information through an established international organization.

- Another common threat that emerged during conversations on this topic was how to build information sharing within the cyber domain. Some recommended focusing on a legal or political agreement signed by willing states on common rules, responsibilities, and commitments. Once agreed upon by national leaders, then each participating state can implement the internal processes by which to share this information. It has to be an institutionalized process and cannot be done in an ad hoc fashion. Others brought up the need for a centralized database for all participating states so as to facilitate transparency and ensure that all actors are fulfilling their commitments. The issue with this is such a center would also require more financial investment by states and more personnel to run it, among other topics that come into focus.

- Logistical ease of information sharing. For the NESA region, there are areas where trust is uncommon among neighbors so initiating an information sharing effort would be a very heavy lift for nation states. It may not be feasible in specific region and willling states may have to move their eyes further away from their own neighborhood for willing partners. Some participants brought up the complications of working with states that may have higher capabiltiies or lower capabilities to your own. Would sharing information lead to states either pushing you for more data or asking you to show technology. Still others brought up the political push that could come from a larger power, like the United States, pushing for such an effort. Such a larger power could serve to help overcome some concerns by regional states due to the fact that a larger power has more capaiblities than most states and if they are willing to cooperate, then the barriers for smaller states become less burdensome.

- Timing was also discussed. All participants pointed out numerous cases revealing the scale by which cybersecurity is vital to each and every state, but that threat has not reached a level where worries about sharing information with another state becomes politically viable. While hoping for different end results, the best way to get to real and substantial information sharing in cyber may have to wait to the frequency and scale becomes much larger than today.

- On the other hand, many participants pointed out that information sharing can start with low hanging fruit – efforts related to cyber that do not risk sensitive information from participating states. One argument propsoed was to cooperate on training future cybersecurity professionals. Exchange students to not only understand how states view cybersecurity, but also to develop a common set of best practices. Still others pointed to common diplomatic efforts on cyber to help bring attention to the threat. Another idea presented was to agree to common standards for basic public-oriented cybersecurity (not related to government operations) that willing countries could agree to implement and cooperate in standing up.

- A final common threat that came up is to focus on practicality. Some states may not be willing to cooperate, others may be willing but find no countries willing to accpet – the situation will vary. There is a lot of diplomatic work that needs to be done. In the meantime, why not allow informal information sharing efforts to proceed by any states willing to perform this. This came up in reference to the trend of minilateralism in the

world today. Willing parties gather and if they agree upon a cooperative effort, then move ahead with it. If unsuccessful, then lessons will be learned form that. If successful, then more states may be willing to join or member states may be willing to intensify their cooperation to more complex elements.

BREAKOUT 1 (Digital)

Trust in Technology:

Each of you has homework to do. We ask you to take a few minutes in the next few days to provide a short response to the following question: How do you define trustworthiness when it comes to digital/online software?

RESPONSES:

The essays by our digital participants were somewhat divided between defining trustworthiness in digital tools between being able to perform as they are designed to and being able to keep outside actors from interfering with users. In broad strokes, the difference between usability and security when it comes to software. Certainly, all participants emphasized both aspects of this divide, but they tended to emphasize one side or the other in responses.

From a government perspective (their respective roles in militaries, government offices, etc.), the security protocols of digital tools are paramount. Access to the entire internet should not always be available to government officials when in their roles and when they use specific digital tools, then they should be closely monitored and/or wholly designed for government use. Some participants pointed out that security is defined differently between private and public entities, so what a government considers security is not necessarily what a private firm sees as secure. Overall, there is immense complexity when it comes to digital tool adoption by governments, for there are examples where designing a more closed system has proven better than a routine commercial alternative. Yet, there are cases when the private sector designs a product that is superior in both use and security to what a government intended. Therefore, creating a stable set of standards is complicated.

BREAKOUT 2 (Digital)

Plugging Gaps in Knowledge:

Now, each of you has homework to do. We ask you to take a few minutes in the next few days to provide a short response to the following question: What would be your first step in the case of a substantial cyberattack within your country?

The essays from digital participants often emphasized diagnostic investigations as a first step in the case of a cyberattack. Such diagnostics can determine the elements that make up the system. Was it an attack on a private or public system? This matters greatly as each operates differently and serves different 'customers. From there, diagnostics can help determine what type of information was on the system and how it was made vulnerable. This could include an analog system that became digital, or a closed system with limited access points to a more open system with multiple access points. You must rely on those with the training to examine the situation and all states have personnel that are trained to do this as quickly as possible.

Furthermore, participants emphasized what comes after initial investigations – actions. Depending on the scenario, a system may need to go offline with available backups initialized as a temporary bridge. This is in the case of a potential critical attack or widespread digital incursion. After getting control of the system, then states may need to consider intensifying their security by training more qualified personnel, building a centralized response institution, diversifying their methodology for responding to cyberattacks, or other elements. Several participants brought up how the public at large can be both a complication from a cyberattack or a resource in responding to one, so all states need to consider how they will interact with the public in such a situation.