Cyber 9/12 Student Challenge

Intelligence Report I

INSTRUCTIONS

Your team will take on the role of experienced cyber policy experts who were invited to brief a task force of European leaders (including heads of state, heads of government, ministers of defense and foreign affairs, directors of intelligence services, and representatives from the private sector) called to address an evolving cyber crisis. This packet contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure and services in Europe. The attacks notionally take place in spring 2018. The scenario presents a fictional account of political developments and public and private reporting surrounding the cyber incident.

You need to provide information on the full range of policy response alternatives available to respond to this crisis, and your team has been tasked with developing four policy recommendations to pass on to the task force. You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform three tasks:

1. **Written Policy Brief:** Write a 500-word brief discussing the key elements and security concerns that the task force must understand. The written task is meant to not only test your team's ability to summarize the scenario, but more importantly to explain the reasons and confidence levels behind your analysis of the key issues and implications of the ongoing cyber incident.
2. **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy options and recommending one to the task force.
3. **Decision Document**: Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The "decision document" will be maximum two single-sided pages (one double-sided page) in length, outlining the team's policy response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Don't fight the scenario.* Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- *Think multi-dimensionally*. When analyzing the scenario, remember to consider implications for other organizations and domains (e.g., private sector, military, law enforcement, information operations, diplomatic, etc.) and incorporate these insights along with cybersecurity.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: **Office of the High Representative of the EU for Foreign Affairs and Security Policy**
Re: **Alarming Cyber Activities Across Europe**
Date: **Friday, 18 May, 2018, 3:53 p.m.**

The Office of the High Representative of the Union for Foreign Affairs and Security Policy has established an international and multi-stakeholder task force and is contacting your team to solicit policy solutions to respond to an evolving cyber incident. The Task Force is made up of German, Belgian, French, and other European national security and foreign policy agencies, as well as private sector representatives. Given the nature of this cyber incident, this group of European leaders wants to assemble a range of possible policy response alternatives before determining a course of action to announce in the next task force meeting at 8:00 a.m. on Monday, 21 May, 2018. Your oral policy brief recommendations must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action.

To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action.

When generating each of your **four** policy response alternatives, the task force requests that you consider the following potentially conflicting interests both at the national level and EU and NATO levels. These are provided as suggested starting points and are not meant to limit your policy responses.

- **Immediate Response vs. Delayed Response**
  What actions should be considered, if any, if there exists a possibility of European agencies' involvement? What actions should to be taken immediately after the incident versus those that should be taken later? How should leverage be maintained?

- **Government Response vs. Private Sector Response**
  What actions taken in response to the reports and incidents should be led by the private sector and what actions should be under the government's leadership? Actions to consider may include public acknowledgements, preventive and preemptive defensive actions, and offensive actions.

- **Explicit Deterrence vs. Implicit Deterrence**
  Should European nations respond openly to deter future attacks? Will the absence of a response – or a covert response – embolden future attackers? How should either option be messaged, if at all? What consideration should be given to escalatory potential of a response meant as deterrence?

- **Direct Response vs. Indirect Response**
  If action is to be taken, should it be a direct or indirect response to the incident? Should those responding act in secret, or reveal their cyber capabilities? Should no action be taken?

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the task force:

- **Tab 1 – Classified EU INTCEN Report**
- **Tab 2 – Email from BVG CEO to German Federal Ministry of Transport and Digital Infrastructure**
- **Tab 3 – The Register News Story**
- **Tab 4 – CLASSIFIED MI6 Memo**
- **Tab 5 – CLASSIFIED NATO Joint Security Awareness Report**
- **Tab 6 – Zeit Online News Story**

Tab 1: Classified EU INTCEN Report

18 May, 2018 08.30 a.m.

MEMORANDUM FOR THE DIRECTOR OF EU INTELLIGENCE AND SITUATION CENTER

SUBJECT: URGENT: Regional Healthcare Outages Due to Cyber Attacks

Healthcare in Antwerp (BE), Ghent (BE), and Grenoble (FR) has been severely impacted by simultaneously occurring cyberattacks yesterday morning. There appear to be no immediate fatalities from the attacks, but current capacity does not meet minimum required levels by public health authorities. If the attacks are sustained, casualties are expect to occur as a result of delays and mistakes in patient care.

On 17 May, between 08.00 and 09.00 a.m. a simultaneous, coordinated attack against seventeen individual healthcare facilities resulted in outages of several medical device and patient records systems. Facilities began using normal downtime procedures for medical records, and called in on-duty physicians to assist with increased staffing associated with manual diasnostics and treatment. Eight hospitals were forced to move patients to other care facilities.

In addition, hospital staff at the ZNA Sint-Elisabeth Hospital in Antwerp reported some nonconformities on patients' identification wristbands and manual patient records. In at least 12 cases, the errors on the wristband included incomplete or wrong patient name, wrong blood type, and wrong patient registration number. The hospital is currently investigating the number of patients affected and whether the attacks against the hospital's networks may have compromised the integrity of patient data or whether these are unrelated incidents.

No group has claimed responsibility for the attack, however EU INTCEN believe with a moderate-high degree of certainty that the ISIS-affiliated Al Durka group carried out the attack. Several technical indicators match Al Durka previous attack patterns; however operational practices and infrastructure have changed, which may indicate a change in leadership, tactical innovation, or another yet-unknown explanation.

The technical sophistication of the attack was very low, and EU INTCEN analysts project that most healthcare systems across member states are vulnerable to the same type of attack. Investigation into the perpetrators and motives behind the attack is still ongoing, and we will update our assessment as more information is uncovered.

ATTRIBUTION – TIES TO AL DURKA

The Al Durka group routinely uses malicious software (ransomware) to attempt to extort healthcare providers. Their normal behavior is to compromise workstations and laptops through spearphishing campaigns. However, in this instance, they appear to have spread through network vulnerabilities inside each healthcare provider. Both the propagation method and the scale of the attack are unprecedented by this actor.

The malicious software used is nearly identical to that known to have been used exclusively by Al Durka in the past. This conclusion is based on multiple conclusive matches for existing indicators of compromise (IoCs) known to be associated with Al Durka. This list of IoCs will be included in a subsequent update. The ransomware is based on Cryptolocker source code leaked on the dark web, to which Al Durka made several modifications unique to the lineage they have developed. Importantly, the command and control infrastructure and bitcoin wallets are not affiliated with known Al Durka activity.

At this time, the differences in operational execution and infrastructure reduce confidence of attribution somewhat. EU INTCEN analysts are examining HUMINT and SIGINT sources for indicators of leadership change, increased collaboration with other groups, sale or leak of their toolkit, or other indicators that may increase our confidence in attribution.

ASSESSMENT OF VULNERABILITIES

Two companies, GR and MacGuessin appear to manufacture all of the systems impacted. Each of these run on the Windows operating system, which is targeted by Al Durka ransomware. In each case so far investigated, the infection vector was identical for each type of device. The GR devices were infected through insecure default passwords, and the MacGuessin devcies were infected through known vulnerabilities.

The following information is representative of each case so far investigated and is provided as background information. It was obtained through public sources and may not apply in all devices or at all of the affected hospitals.

- The affected GR devices are designed with publicly knonw maintenance credentials, which allow unauthorized parties to gain access to the underlying Windows operating system. These credentials can be changed in newer versions of GR devices, however, most healthcare facilities do not change them. GR represents approsimately 25% of the European market for diagnostic imaging devices like the ones affected, across Europe.
- The affected MacGuessin devices contain software defects in its version of the Apache Struts library that allow an unauthenticated attacker to gain access to the underlying Windows operating system. These vulnerabilities have been known since early 2014, and exploits are widely available and reliable. An update exists for the Apache Struts framework, which MacGuessin has incorporated into updated software for the device. However, many hospitals have not installed the updates. MacGuessin represents about 12% of the European market for patient records systems like the ones affected, across Europe.

At this time, we estimate that many – but not all – healthcare providers in member states have similar equipment. However, we do not have precise counts, and we do not know whether those systems are vulnerable to a similar exploit.

Classified by: DIREUINTCEN [EXERCISE]
Reason: 1.5(c)
Declassify on: 25X

Tab 2: Email from BVG CEO to German Federal Ministry of Transport and Digital Infrastructure

PRIORITY: **HIGH**
From: Dr. Leticia Löfgren, Chief Executive of Operation, Berliner Verkehrsbetriebe
Sent: Wednesday, May 16, 2018 9:35 AM
To: Hans Weber, Political Staff, Policy Planning and Coordination Directorate-General, Federal Ministry of Transport and Digital Infrastructure, Federal Republic of Germany

Dear Hans,

I'm writing to inform you about a hacking incident at BVG that affected the functioning of several U-Bahn train lines. Early yesterday morning, a ransomware attack took ticket machines for Berlin's U-Bahn system offline forcing them to display an "Out of Service" message. It disrupted our internal computer system and email but did not affect the actual running of the transit system. This resulted in a small loss of revenue to the system, less than 80,000 EUR, and a capital expense of 100,000 EUR to pay the ransom.

At 07:47 am, we received a message from a group calling themselves NovAnoN demanding a ransom of 100 bitcoins (approximately 100,000 EUR) in return for access to our systems by the end of the day. NovAnoN claimed to have encrypted all our data using a special key that will be revealed to us only on payment of the ransom. We allowed passengers to ride for free till around 5:00 pm hoping that we will be able to arrive at a better solution. However, our IT department was unable to get our systems back to normal by then. We paid them the ransom at 6:00 pm, received the decryption key and immediately alerted the authorities. We have managed to get our systems back to normal today and should not face any problems.

Our IT department says that we were not targeted for this attack but just happened to fall into a wide net cast by the group. The root cause of infection appears to be unpatched software, however we are still investigating how the initial intrusion occurred. As this attack touched a large number of systems responsible for daily operations, we will issue a public statement about it tomorrow.

I just wanted to make sure you were up to date on the issue in case you are questioned about it by the press. Please let me know if you have any questions about this.

Sincerely,
Leticia

Dr. Leticia Löfgren

Chief Executive of Operation
Berliner Verkehrsbetriebe
Holzmarktstraße 15-17 | 10179 Berlin
T: +49 176 8944 849| E: lloefgren@bvg.de
@BVG_Kampagne | www.bvg.de

Tab 3: The Register News Story

The Register®
Biting the hand that feeds IT

DATA CENTER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

Global Health System at risk from hackers

Patients and physicians peeved, as hospitals buy more bitcoin instead of fixing the problem

23 Jan 2018 at 11:24, John Leyden

Almost two years after Hollywood Presbyterian Hospital was shut down by hackers, the California healthcare provider has recovered control of its facility, but not its reputation. “Each time a new wave of ransomware shuts down hospitals, our name gets mentioned yet again,” says Brianna Knopf, Medical Director of the beleaguered hospital. Next month, the facility will change its name to Kaiser Hollywood Hospital following an acquisition by Kaiser Permanente.

The-artist-soon-to-be-formerly-known-as Hollywood Presbyterian Hospital was the first but not the last healthcare facility to be shuttered by ransomware. In 2016 alone, there were nearly 100 reported major incidents involving hospitals being hacked. Tens of millions of patients’ records fell into the hands of nefarious no-gooders. In Washington DC in March 2016, just a few days before the Nuclear Security Summit gathered heads of state from around the world, the MedStar system – along with its Level 1 trauma centers – were shut down. And later in October the same year, several of the UK National Health Service hospitals were forced to cease operations after a ransomware attack.

Ransomware has become big business in the past twelve months. In 2016, the FBI reported global ransomware payments would exceed $1 Billion USD. According to sources within Downing Street, NHS spent nearly 350 Million GBP in increased health services costs during ransomware attacks. The source declined to comment whether the government has paid any ransoms, however, a consultant for a large security firm who has investigated such attacks said that he has seen it happen.

To the concern of many counterterrorism experts, cybersecurity companies have witnessed a rapid increase in terrorist groups’ use of ransomware against healthcare facilities and other organizations particularly in Syria, Iraq, and Indonesia over the past few months. The groups have reportedly used the funds collected to finance their operations, and many analysts warn that when used against hospitals, ransomware could also be used to compromise patient care and steal or manipulate confidential patient data.

Hospitals are uniquely vulnerable to such attacks. They have a large number of high cost, low security medical devices that may be years out of date on security updates. A hospital IT staff member the Register spoke with said that many of the hospitals systems – including medical devices – aren’t sold or supported any longer by the company that made them. And even when an update is available, the medical device maker charges fees for the “upgrade,” and requires a certified maintenance specialist install it for yet another high fee. On the plus side, he said, his facility had just completed their migration from Windows XP (which ended life in 2014 – 12 years after it was introduced), to Windows 7 (a 9 year old operating system which will cease to be supported in only two years).

Preliminary analysis shows that there have been few fatalities despite the widespread issues. Physicians, Christian Dameff and Jeffrey Tulley presented preliminary research at a CyberMed Summit event held in

June 2017 that there is a twelve per cent increase in mortality rate during ransomware events. The physicians said the dataset was small, however, because most hospitals refuse to share such information. In one high-profile case, two British soldiers died in Mosul, Iraq in April 2017 after their vehicle was ambushed in a roadside bomb and the Army hospital in Mosul was allegedly unable to operate due to a ransomware outbreak. However, Army spokespersons have repeatedly denied that ransomware played any part in the soldiers' death.

Tab 4: CLASSIFIED MI6 Memo: Assessment of ISIS Status and Likely Future Action

SECRET INTELLIGENCE SERVICE MI6

22 March, 2018 14.45

MEMORANDUM FOR THE DIRECTOR OF MI6

SUBJECT: Assessment of ISIS Current Status and Future Actions

Following the surprisingly quick fall of the Old City of Mosul in June 2017, ISIS' presence in Iraq effectively evaporated. The remaining core fighters fled to Raqqa to reinforce their final major urban center, leaving only fringe groups in Iraq without any effective command and control. While the Government of Iraq still has not eliminated all remaining insurgent fighters and groups, they will mostly turn to local criminal actions rather than supporting the ISIS cause. They will be unlikely to receive any further funding or support from the remnants of the ISIS organization now contained to Syria.

The remaining elements of ISIS still in Raqqa are likely to be the most fanatical and battle hardened. The recently announced, but not yet commenced, operation to retake Raqqa will likely be drawn out and result in significant casualties. ISIS has effectively been contained to Syria and their capabilities has been severely degraded. Nonetheless, they will continue to inspire other groups to act, and the remnants of their support network will continue to pursue similar goals regardless of command and control from ISIS hierarchy. Moreover, the remaining ISIS elements will be forced to be more creative in their attempts to fund their remaining forces.

Resource Constraints

One of the greatest organizational strengths of ISIS was its diversified approach to generating revenue. Once hailed as the worlds "richest terrorist group", they enriched themselves through seizure of government property, oil wells and stockpiles, taxing of local populations and the sale of antiquities. At their height, they could attract recruits through the provision of generous salaries and provide public services to the population in their controlled territories.

As they have lost territory, the group has also lost most of its traditional sources of income. ISIS leaders have reportedly reduced spending on salaries and services, but are unable to generate significant revenues

to support their remaining forces. This is driving ISIS to seek new and innovative sources of revenue. As they are effectively contained in their remaining enclave, they are likely to leverage their broader global networks. Like other terrorist groups who have turned to crime to support their cause, renting the services of their armed groups and smuggling networks will be most likely to generate new income. As foreign fighters return to their home countries, they will likely continue to support ISIS cause through criminal activity. This is most likely amongst populations in poorly governed or restive regions such as Chechnya and the Uighur regions of China. Those who return will be able to recruit locals support in the largely untapped Muslim populations there.

One unique advantage ISIS has compared with other terrorist and trans-national criminal groups is their cyber capabilities, and MI6 analysts expect the group to increasingly turn to cyber crime to raise sufficient funds to sustain its operations. At its height, ISIS's cyber capabilities were formidable, and the group still retains significant social media networks that could be repurposed for information operations. ISIS also has a cadre of highly capable hackers who have acquired sophisticated tools from supporters in Russia and China, and purchasing leaked tools on the dark web. With a global network of supporters, MI6 analysts expect that ISIS could easily rent or sell cyber-attack or espionage capabilities to the highest bidder.

Future Actions

ISIS leadership continues to seek international legitimacy by drawing Western nations into a conventional confrontation in Syria. It will continue to seek this through ongoing attacks against high profile Western targets, in order to motivate Western populations into pressuring their governments to intervene militarily in Syria. While their resources to undertake sophisticated attacks has been severely diminished, they will continue to seek creative and innovative ways to attack the West. MI6 expects the group to remain a highly dangerous threat, particularly as they become more desperate and seek new partners.

Classified by: MI6
Reason: 1.5(c)
Declassify on: 25X

Tab 5: CLASSIFIED NATO Joint Security Awareness Report

NORTH ATLANTIC TREATY ORGANIZATION

JOINT SECURITY AWARENESS REPORT (JSAR-18-030-01A)

Original release date: May 6, 2018 | Last revised: May 7, 2018 08:15

SUBJECT: EMERGENCE OF AL DURKA BRIGADE

Recent monitoring of ISIS cyber operatives has identified the emergence of an offshoot of its 'Cyber Caliphate' which self-identifies as the Al-Durka Brigade. In comparison to the broader goals of the Cyber Caliphate, the Al-Durka Brigade appears to be narrowly focused on enabling new terrorist attacks and generating online revenue for the remaining ISIS force.

The group has undertaken a range of online activities, from low level DDOS attacks to online scams on both the Clear and Dark nets. They have demonstrated a range of hacking tools, but the sophistication to date has not been significant. They have been detected as having been involved in several online transactions, both selling cyber services and tools as well as seeking to purchase more advanced ones. This action has been particularly significant with known Russian criminal groups in possession of sophisticated hacking tools. These connections may have been facilitated by Chechen fighters known to have joined ISIS.

Of particular note, the Al Durka Brigade has demonstrated a disproportionate interest in acquiring ransomware tools, medical device instruction manuals, and stolen hospital network diagrams. It is currently assessed that this is likely to be an attempt to diversify sources of income generation. While the Al Durka Brigade has utilized a range of

online scams, fraud and identity theft to generate revenue, they have recently undertaken a number of significant ransomware attacks against small private-sector organizations and high-net worth individuals in North Africa and Turkey. There are also indications that the Al Durka Brigade may have been engaged in espionage activities for a State actor, likely to be North Korea.

While it is assessed that the majority of the Al Durka Brigade consists of former ISIS fighters, coalition forces' HUMINT sources indicate that the group may be seeking to recruit IT professionals from Europe, particularly those from Global 500 companies with experience in business management or in administering large corporate networks.

It is assessed that the Al Durka Brigade will seek to expand their capabilities and service offerings through exploiting low cost, low hygiene devices to create botnets for extortion and targeting high consequence devices to cause high damage and higher ransomware takes.

Tab 6: News Story: "The New Rise of the Black Bloc in Cities and in Cyberspace"

Anarchism in Europe

The New Rise of the Black Bloc in Cities and in Cyberspace

For days, protesters in major cities across Europe have been fighting with the police. The waves of violence have shifted from groups traditionally associated with left-wing opposition to state power and capitalism into former strongholds of the right-wing populist movements in France, the Netherlands, and elsewhere. At the same time, a new anarchist group gains traction in cyberspace.

Lisa Steffen, Berlin May 17, 2018

Protests first erupted in the evening of May 12 in Toulouse, France, where a group of young people dressed all in black gathered in the streets, throwing rocks at parked police vehicles. The group was heard shouting slogans opposing the French government's recent, heavy cuts on government welfare programs. As police fired tear gas to disperse the crowd of about 200 protesters, smaller groups went on a rampage in other parts of the city, smashing windows and setting fire to cars and trash cans.

There were similar scenes that evening in Almere, the Netherlands: Some 150 masked protesters in head-to-toe black clothing charged through the Dutch town, formerly known as a stronghold of right-wing, anti-immigrant candidate Geert Wilders who suffered a bitter defeat in the March 2017 elections. The crowd was younger than often seen in the Freedom Party rallies, holding signs and chanting against 'state oppression' of the Dutch working class and denouncing perceived preferential treatment of recent immigrants and refugees. From Almere and Toulouse, the protests quickly spread to cities across Europe including Athens, Maastricht, Nice, and Dresden, turning into violent riots with multiple arrests and an estimated €700,000 in damage in Toulouse alone.

The ‘black bloc’ protests follow months of smaller demonstrations and political turmoil in France, the Netherlands, and Germany where far-right parties and candidates suffered electoral losses in presidential and parliamentary elections in 2017. While the populist movements had gained great momentum since ‘Brexit’ and the election of Donald Trump as the US president – developments that caught many establishment politicians off guard in 2016 – the far-right parties’ losses in Europe left the movement fractured and dissolved.

Many young supporters of Marine Le Pen of the French Front Nationale, Geert Wilders of the Party of Freedom, and Frauke Petry of the Alternative for Germany (AfD) quickly aligned themselves with new forms of populist opposition movements. Particularly in the areas hardest hit by youth unemployment, the countries soon witnessed a visible uptick in ‘black bloc’ tactics of protests: black clothing, ski masks, charging through the streets in public demonstrations, provoking police, and destroying property. Pockets of the black bloc protesters disrupted peaceful protests against unemployment, government austerity measures and cuts on welfare programs, and immigration in the early months of 2018. This week’s riots represent a new high for the anarchist groups.

While the black bloc has vandalized Europe’s streets, intelligence agencies across the continent have become alarmed by the simultaneous rise of what is described as an Anonymous splinter group “NovAnoN.” While Anonymous is often seen as a loosely associated international network of hacktivists, its offshoot NovAnoN is considered by many experts to have a more centralized command structure and established funding structure. This new group has defaced government websites with messages supporting the black bloc protests and taken it to Twitter to announce their desire to “splinter Europe into kindling and watch it burn.” NovAnoN is also suspected to be behind the number of fake news articles that emerged in outlets such as *Firebrand Left*, *Last Line of Defense Europe*, and *LinkBeef EU,* falsely claiming police brutality against the May 12 protesters in Toulouse. The articles and NovAnoN-affiliated Twitter accounts played a key role in fueling anger and spreading riots from Toulouse to other cities.

Tuesday’s arrest of one of the NovAnoN members by the Czech police revealed that the group has succeeded in attracting very high-profile, high-skilled members to join its ranks: Ivo Rusnok, 47, who was arrested in Brno on May 15, is the former IT director of the US-based Fortune 500 company Berkshire Holdings Ltd and a visiting scholar at Carnegie Mellon School of Computer Science. Rusnok was also a prominent supporter of the 2011 Occupy Wall Street protest movement, raising awareness for economic inequality worldwide. Rusnok remains in Czech police custody. The investigation into his role in some of the recent hacks claimed by the splinter group NovAnon is ongoing, but his arrest raises serious concerns for European law enforcement agencies.

Cyber 9/12 Student Challenge

Intelligence Report II

INSTRUCTIONS

Your team will take on the role of experienced cyber policy experts who were invited to brief a task force of European leaders (including heads of state, heads of government, ministers of defense and foreign affairs, directors of intelligence services, and representatives from the private sector) called to address an evolving cyber crisis. This packet contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure and services in Europe. The attacks notionally take place in spring and summer 2018. The scenario presents a fictional account of political developments and public and private reporting surrounding the cyber incident.

You need to provide information on the full range of policy response alternatives available to respond to this crisis, and your team has been tasked with developing four policy recommendations to pass on to the task force. You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform two tasks:

4. **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy options and recommending one to the task force.
5. **Decision Document**: Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The "decision document" will be a prepared form, maximum of two single-sided pages (one double-sided page) in length, outlining the team's policy response options, decision process, and recommendations. This document will allow the judges to familiarize themselves with the proposed policy options in an efficient manner.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Don't fight the scenario.* Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g., private sector, military, law enforcement, information operations, diplomatic, etc.) and incorporate these insights along with cybersecurity.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: **Office of the High Representative of the EU for Foreign Affairs and Security Policy**
Re: **Increasing Cyber Activities across Europe**
Sent: **Monday, June 18, 2018 8:42 PM**

The date is June 18, 2018, and your team has recently presented policy recommendations to the European task force formed by the Office of the High Representative of the Union for Foreign Affairs and Security Policy. Since then, we have witnessed increasing cyber activities across Europe, described as an "imminent threat" to public safety in many countries in the region. Given the growing urgency of the situation, the chairman of the task force has asked your team to consider the latest information available and develop additional policy response options to present at the next task force meeting tomorrow morning, Tuesday June 19, 2018 at 9:00 a.m.

To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action.

When generating each of your **four** policy response alternatives, the task force requests that you consider the following potentially conflicting interests both at the national level and EU and NATO levels. These are provided as suggested starting points and are not meant to limit your policy responses.

- **Immediate Response vs. Delayed Response**
  What actions should to be taken immediately after the incident versus those that should be taken later? How should leverage be maintained?
- **Government Response vs. Private Sector Response**
  What actions taken in response to the reports and incidents should be led by the private sector and what actions should be under the government's leadership? Actions to consider may include public acknowledgements, preventive and preemptive defensive actions, and offensive actions.
- **Unilateral Response vs. Multilateral Response**
  Should there be a multilateral response or unilateral response? What about international organizations like the United Nations, the World Health Organization, the European Union, and NATO?
- **Diplomatic Response vs. Military Response**
  Should a military or diplomatic response to the incident be taken? How can international partnerships and allies be involved?

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the task force:

- **Tab 1 – INTERPOL Code Orange Notice to domestic law enforcement**
- **Tab 2 – EU Observer Article**
- **Tab 3 – NATOSource Tweet**
- **Tab 4 – CLASSIFIED DGSI Memo: Assessment of NovAnoN's Transnational Network**

Tab 1: INTERPOL Code Orange Notice to domestic law enforcement

Requesting Country: Belgium

Date and Time of Publication: June 18, 2018, 10:37 a.m.

INTERPOL ORANGE NOTICE

IMMINENT THREAT

PATIENT CARE HELD HOSTAGE

Ransomware attacks on hospitals across Europe pose acute threat to public safety

There is an emerging, imminent threat to public health sector across Europe. Criminal groups have taken control over clinical computer systems and medical devices in several hospitals in at least four European countries, holding these hospitals for ransom. The attackers are targeting healthcare delivery organizations and willfully endangering patient safety to increase likelihood and price of ransomware payments. This represents a shift in technique that greatly increases danger to public safety. Recent Intelligence suggests coordinated attacks are being planned for multiple cities throughout Europe over the coming months.

INTERPOL has received numerous reports of conflicts between police agencies and public health officials during such incidents. Hospital staff's actions to restore healthcare service have interfered with chain of custody and forensic integrity required by police departments. INTERPOL advises that police forces coordinate with their own national agencies for guidance on handling such conflicts. INTERPOL has established a task force to investigate the situation, and is offering technical support to police forces through a group specifically trained on law enforcement investigations of ransomware incidents.

Threat

- Coordinated ransomware attacks on hospitals and healthcare facilities ongoing across Europe using open source malware.
- Since June 15, 2018, attacks have been reported on 28 healthcare facilities in Belgium, France, Austria, and the Netherlands.
- Affected hospitals struggling to get back online, severely affecting patient care. Unconfirmed reports of at least 10 patient deaths in Austria and Belgium due to overwhelmed resources are being investigated by domestic law enforcement.
- High impact combination of hospital ransomware-kinetic attack as in Russia on June 16 could be replicated. According to Russian law enforcement, it is currently unclear whether the attacks were coordinated, and who was behind them.
- Links between all attacks currently being investigated.
- Intercepted communications indicate high possibility of a large-scale attack in coming months with several groups now likely actively using open source malware kit.

Actor(s)

- Anarchist group NovAnoN suspected by law enforcement in all affected countries.
- Leaderless organization similar to, and some members with ties to Anonymous, likely centralized in Central and Eastern Europe and known for information operations.
- Al-Durka Brigade, splinter group of ISIS Cyber Caliphate, shifting aims of cyber attacks from large-scale destruction to monetization.
- NovAnoN and Al-Durka seem to have reached a symbiotic relationship, rather than a competitive one, with NovAnoN the primary group targeting healthcare, and Al-Durka focusing on high net-worth individuals.

Background

Ransomware in healthcare facilities has become an increasingly familiar threat across Europe. Hospitals are considered easy targets for monetization, as they tend to have lower levels of cybersecurity and the urgency to pay is higher.

In May this year, similar attacks shut down 17 healthcare facilities in Belgium and France. Belgian and French authorities now believe malware

used by the ISIS-affiliated Al-Durka Brigade was harvested from a victim system by NovAnoN with a modified configuration file. NovAnoN has since acquired capabilities to create their own ransomware variants based on the leaked Cryptolocker source code, in a similar way as Al-Durka originally did.

Also in May, ransomware shut down the German U-Bahn system when it got caught in a wide net cast by NovAnoN. NovAnoN succeeded in monetizing the attack and gained EUR100,000 in BTC. Interpol believes that this success and financial gain prompted NovAnoN to explore ransomware capabilities further while Al-Durka's success in disrupting the healthcare sector inspired NovAnoN's targeting of hospitals.

Technical Information

Interpol analysts believe that the strain of ransomware in the recent attacks that occurred across Europe is a variant of the open source ransomware kit, based on the previously leaked Cryptolocker source code. Ransomware is commonly spread through various infection vectors, including browser exploit kits, drive-by downloads, malicious email attachments, default passwords, and known network vulnerabilities.

The vulnerabilities exploited in these attacks have been publicly known for several years. One exploit targeted CVE-2008-4250, a vulnerability in the Microsoft Windows operating system known since 2008 that gave the attacker full control over workstations, servers, and medical devices affected. One exploit targeted CVE-2014-7912, a vulnerability in the Android operating system known since 2014 that gave the attackers full control over medical devices affected. In contrast to so-called 0-day vulnerabilities, exploits for the ones used in the June attack were reliable and widely available, without any specialized knowledge or training. The Medical Device Vulnerability Intelligence Program for Evaluation And Response (MD-VIPER) database reports that as many as one-in-six networked medical devices is affected by these two known vulnerabilities.

The links between the malware demonstrate a gradual progression and pattern of feature accretion around a central code base. New functionality is implemented and old features are deprecated as needed, but many core functions are retained.

The minor alterations such as beacon domains and different filenames would allow new variants to evade many signature-based detection systems using signatures developed from previous samples without the time-consuming process of rewriting the entire code base for each campaign. These capabilities, along with polymorphic repacking, anti-forensics,

and other techniques, have been introduced into NovAnoN's code base from other open source code. This new practice demonstrates a slight elevation in NovAnoN's operational sophistication that brings a huge increase in their technical capabilities.

Interpol analysts have previously observed that threat groups who deploy targeted ransomware do so only after they have established and maintained a foothold in the victim's environment for weeks to do reconnaissance and discover where and what valuable data is being stored by the victim.

Some ransomware variants apply an urgency to ransom payments. For example, Jigsaw deletes a portion of the encrypted files every 60 minutes and each time the infection restarts. Other variants increase the ransom if it is not paid within a certain timeframe. These tactics focus victims' attention on prompt payment to avoid data loss rather than on alternative options of data recovery. These same tactics have been adopted by NovAnoN because of their effectiveness on healthcare delivery decision-makers.

Implications for Clinical Healthcare

These attacks have particularly severe implications for healthcare providers. Healthcare is one of the most interconnected industries, yet also tends to have the fewest IT resources per staff, resulting in a much higher incidence of ransomware infection. In addition, the impact to human life and public safety are extreme, including localized and widespread loss of life. This combination of high dependence, high connectivity, low resources, and high consequences, make hospitals highly susceptible to ransomware crime.

Three classes of technology pose the most acute risks in hospitals: medical records systems, diagnostic equipment, and treatment devices. These systems, taken together, give a high degree of leverage, allowing a single caregiver to treat 10-20 times more patients than would otherwise be possible.

- Medical records systems contain the collected information about patients. Physicians increasingly – though not completely – rely on information contained for patient care, particularly in emergency situations when the patient cannot speak and when paper files are unavailable. When these systems are unavailable, time to diagnose patients can be extended by hours, and require greater work effort and cost.
- Diagnostic systems assist physicians in understanding patients' underlying conditions, as a precursor to treatment. These systems

automate many manual processes, give real time feedback to care givers, and can alert on dangerous changes in conditions. X-Ray, MRI, CT Scanning, laboratory testing, EKG, and other systems all rely on computer and network technology.

- Treatment devices significantly reduce resources and decrease variability in treatment. Drug infusion pumps, dialysis machines, respirators, pharmaceutical dispensers, and other technology has drastically improved quality of care over the past 30 years.

When these systems are impacted, hospital resources become exhausted quickly, delivery timelines increase, and consistency of care suffers. In one such recent attack that lasted 36 hours, the normal physician and nursing staff of 122 had to be increased to 300, drawing all on-call and off-duty personnel currently on staff, at the targeted facility, as well as two others nearby. The hospital replaced affected medical devices with spare units, which were quickly disabled by the "network worm" capability of the ransomware. Confusion with system outages was compounded by unfamiliarity with hospital processes on the part of the new physicians, and six patients were improperly treated, resulting in four near-fatal conditions. As physicians raced to save one life, another patient in worse condition could not be treated and expired. During the 36 hours of this state, all incoming ambulances were redirected and the hospital sent non-critical patients to other facilities. The incident ended when the national healthcare authority paid EUR250,000 in bitcoin, after suffering over 1 Million Euro in losses. Statistical analysis shows that patients suffered an additional 2% mortality rate during the event.

Intergovernmental intelligence briefings have shown grave concern among the heads of medicines regulatory agencies across Europe and North America – including the US FDA – that a sustained event could pose an imminent threat to those countries' public health systems.

Preparation and Mitigation of Future Attacks

INTERPOL recommends that all hospitals follow recommendations developed by the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), the National Health – Information Sharing and Analysis Center (NH-ISAC) and the Multi-State Information Services and Sharing Center (MS-ISAC) in preparing for and mitigating future attacks:

Preparation Beats Mitigation: It is easier to prevent an infection or an attack than it is to clean one up. Best practice is to focus on defense and utilize several layers of security including:

- *Operating systems, medical devices and antivirus software should be kept up to date*
- *Employee education*
- *Files should be backed up and available to reload if necessary – backups should be stored in the cloud or on drives separate from the network*
- *Manage the use of privileged accounts – administrator level access should be minimized*
- *Have a plan and exercise it; work in concert with outside providers, such as biomedical contractors and device makers.*

Attack Mitigation: Being prepared is essential to reduce the effects of a ransomware attack. Here are tips on how to address ransomware post-attack:

- *Isolate the infected system from your network.*
- *Restore files by using files from regularly maintained backups.*
- *Report the infection to domestic law enforcement and Interpol*
- *Participate and share in an information sharing organization, such as your industry ISAC.*

Recommendations: Be aware of how your network is configured and what software you use on a regular basis. By knowing what your system looks like and how it works, you will be able to identify problems when they occur. Here are some key recommended steps:

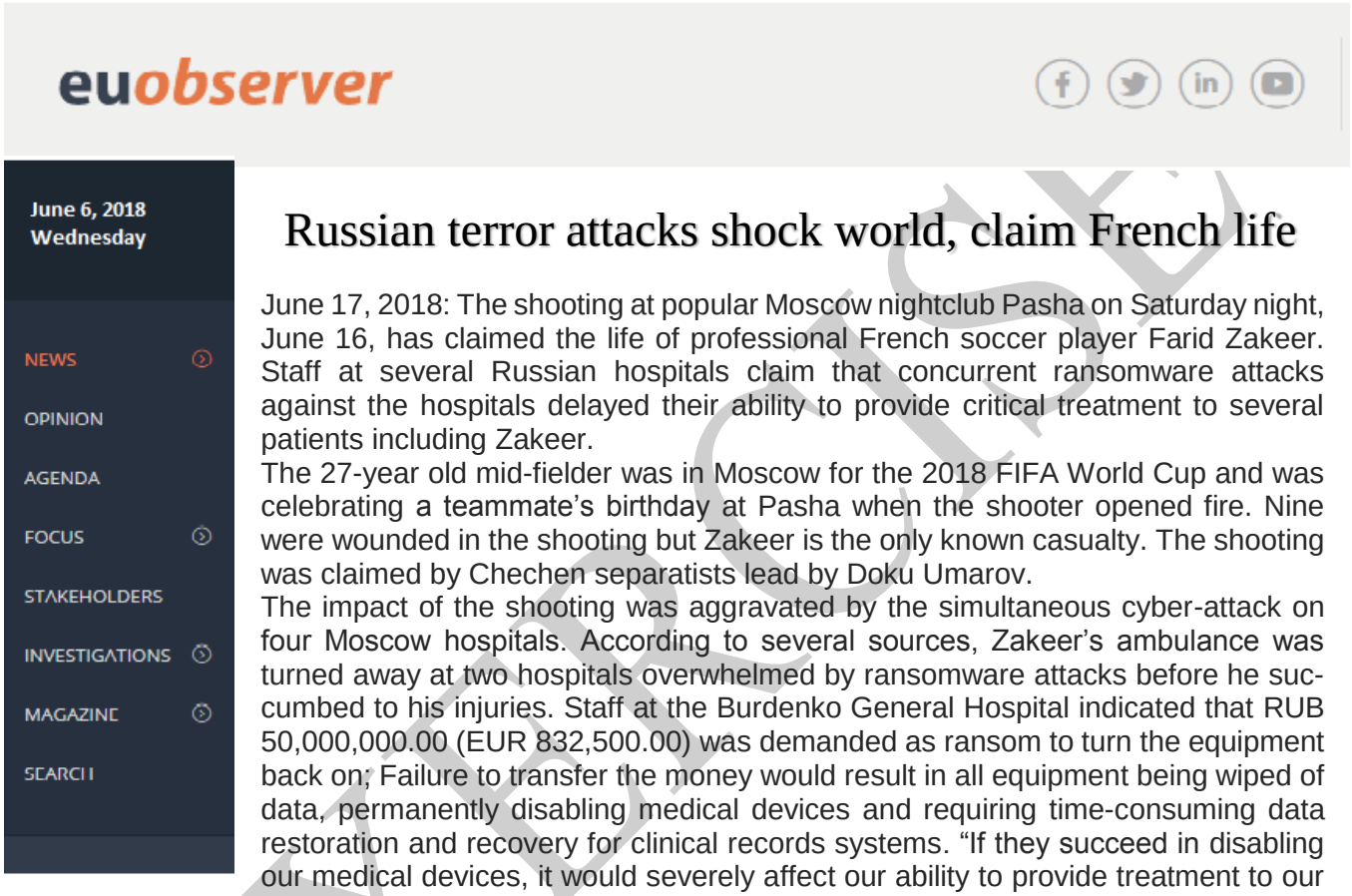
- *Perform regular backups of all systems*
- *Know what is connected to and running on your network*
- *Use (but don't rely solely on) antivirus and anti-spam solutions*
- *Disable macro scripts in Office*
- *Restrict internet access, particularly to clinical devices*
- *Participate in cybersecurity information sharing organizations*
- *Create a solid business continuity plan*

Attachment: List of affected hospitals by country

DATE	HOSPITAL AFFECTED	STATUS
FRANCE		
June 1	University Hospital of Montpellier	Affected systems taken offline – Manual operations
June 1	Nice University Hospital, Nice	Affected systems taken offline – Manual operations
June 1	Hôpital Les Broussailles, Cannes	Affected systems taken offline – Manual operations
June 1	Grenoble University Hospital, Grenoble	Affected systems taken offline – Manual operations
June 1	American Hospital of Paris, Paris	Ransom paid – Decryption key received
June 1	Hôpital Suisse de Paris	Ransom paid – Decryption key received
June 1	Centre hospitalier Chateau-Thierry	Ransom paid – Decryption key received
BELGIUM		
June 1	CHU Saint-Pierre, Brussels	Ransom paid – Decryption key received
June 1	Clinique Saint Jean, Brussels	Affected systems taken offline – Manual operations
June 1	Universitair Ziekenhuis Leuven	Affected systems taken offline – Manual operations
June 1	Institut Jules Bordet, Brussels	Affected systems taken offline – Manual operations
June 1	AZ St.-Elisabeth Herentals	Affected systems taken offline – Manual operations
June 5	Queen Fabiola Children's University Hospital, Brussels	Critical systems affected – assistance requested
June 5	Hôpital Erasme - Anderlecht	Critical systems affected – assistance requested
AUSTRIA		
June 5	Landeskrankenhaus (LKH) - Universitätsklinikum Graz	Critical systems affected – assistance requested
June 5	Landesnervenklinik Sigmund Freud, Graz	Critical systems affected – assistance requested
June 5	Krankenhaus der Barmherzigen Brüder Eggenberg, Graz	Critical systems affected – assistance requested
June 5	Unfallkrankenhaus Meidling	Critical systems affected – assistance requested

June 5	Vienna General Hospital	Critical systems affected – assistance requested
June 6	Wiener Privatklinik, Vienna	Critical systems affected – assistance requested
June 6	Wilhelminenspital, Vienna	Critical systems affected – assistance requested
NETHERLANDS		
June 6	VU University Medical Center VU medisch centrum (VUMC), Amsterdam	Critical systems affected – assistance requested
June 6	Maasstad Ziekenhuis, Rotterdam	Critical systems affected – assistance requested
June 6	University Medical Center Groningen Universitair Medisch Centrum Groningen (UMCG), Groningen	Critical systems affected – assistance requested
June 6	Academic Hospital Maastricht Academisch ziekenhuis Maastricht (AZM), Maastricht	Critical systems affected – assistance requested

Tab 2: EUObserver Article



euobserver

June 6, 2018
Wednesday

NEWS
OPINION
AGENDA
FOCUS
STAKEHOLDERS
INVESTIGATIONS
MAGAZINE
SEARCH

Russian terror attacks shock world, claim French life

June 17, 2018: The shooting at popular Moscow nightclub Pasha on Saturday night, June 16, has claimed the life of professional French soccer player Farid Zakeer. Staff at several Russian hospitals claim that concurrent ransomware attacks against the hospitals delayed their ability to provide critical treatment to several patients including Zakeer.

The 27-year old mid-fielder was in Moscow for the 2018 FIFA World Cup and was celebrating a teammate's birthday at Pasha when the shooter opened fire. Nine were wounded in the shooting but Zakeer is the only known casualty. The shooting was claimed by Chechen separatists lead by Doku Umarov.

The impact of the shooting was aggravated by the simultaneous cyber-attack on four Moscow hospitals. According to several sources, Zakeer's ambulance was turned away at two hospitals overwhelmed by ransomware attacks before he succumbed to his injuries. Staff at the Burdenko General Hospital indicated that RUB 50,000,000.00 (EUR 832,500.00) was demanded as ransom to turn the equipment back on; Failure to transfer the money would result in all equipment being wiped of data, permanently disabling medical devices and requiring time-consuming data restoration and recovery for clinical records systems. "If they succeed in disabling our medical devices, it would severely affect our ability to provide treatment to our hundreds of patients," said a doctor at Burdenko. Burdenko Hospital's CEO, Nikolay Bazarov, has appealed to the Russian government to pay the ransom on their behalf. Russian government officials could not be reached for comment.

euobserver

June 6, 2018
Wednesday

NEWS
OPINION
AGENDA
FOCUS
STAKEHOLDERS
INVESTIGATIONS
MAGAZINE
SEARCH

While it has not been established that both the shooting and ransomware was executed by the same threat actors, it could be a sign of things to come. Security experts warn of more such hybrid attacks, especially from high-impact adversaries like terrorist and extremist groups.

Ransomware attacks against the healthcare sector have become common over the last decade, but this combination of ransomware and wiper attacks has been relatively rare. Since the famous Hollywood Presbyterian ransomware attack in the US in early 2016, there have been more than 100 incidents of hospitals being hacked on both sides of the Atlantic

Tab 3: NATOSource Tweet

Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

Tab 4: CLASSIFIED DGSI Memo: Assessment of NovAnoN's Transnational Network

30 May, 2018 10.15

MEMORANDUM FOR DIRECTOR OF THE DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE

SUBJECT: Assessment of NovAnoN's Transnational Network

The group NovAnon is assessed to present a real and imminent threat to peace and security in France and other countries particularly in Central and Eastern Europe. The group has undertaken increasingly violent political protests that have been occurring over the past six months across Europe, including in Paris, Lyon and Toulouse. It is assessed that the group contains numerous known anarchists as well as political activists previously involved in recent political campaigns, particularly those associated with the Presidential bid of Marine Le Pen of Front Nationale. The members are assessed as being highly active across France, and Europe more broadly. The group was involved in the attacks on German U-Bahn lines on May 15, 2018 and based on the assessment by the Direction générale de la sécurité intérieure can be expected to undertake further virtual and real-world terrorist and criminal activity.

Structure and Intent

NovAnoN appears to be a manifestation of several sub-cultures than manifest both virtually and in real life. The group is structured in tiers and various functions are carefully compartmentalized. The core group is assessed to be relatively small, with only 8-10 members. Each member has a specific responsibility and their actions are completely separated from the others, in a similar organizational structure of many terrorist and trans-national criminal groups. That member then manages a subordinate cell that carries out compartmentalized functions, and so on. There is also likely to be functional redundancy built into the structure. While inefficient, this organizational design protects the wider group from compromise by law enforcement and limits the damage of any one cell being infiltrated. It also means that at times the groups may work at cross purposes, or even undermine their own efforts due to ignorance of the actions of other cells activities. This is particularly important as certain elements of the group – such as those protesting

publicly, are liable for arrest. The group cannot risk compromising its revenue generating cell being implicated directly in such actions. It is assessed that at a minimum the group has compartmentalized capabilities dedicated to revenue raising, online activism, real-world activism, strategic communications and internal security, with broad coordination occurring through the central cell.

It appears that members in the various tiers of the group met on different websites and virtual communities. It is likely that most met through political and anarchist forums, but there are also indications that others may have met through online gaming communities, anti-capitalist, racist, and conspiracy forums and through online illicit trading, such as darknet drug markets. The group has publicly stated their political ideology as being anarchist and anti-globalization in nature, but general dissatisfaction and greed must also be considered key motivations. It is highly likely that a high number of the more sophisticated actors are involved in the search for illicitly gained profits.

NovAnoN appears to have learnt lessons from a range of previous actors, from LulzSec to ISIS and their Cyber Caliphate, in shaping their approach. This means they likely understand the need to shape the public narrative, how to shape public perception through media manipulation, the power of tailored messaging to different groups and the need to gain and retain sophisticated capabilities through monetary means. This means that the need to continually generate funding is of high importance to this group and linked online transactions should be considered as an indicator of future action.

Financing

The group appears to be financing its activities primarily through online transactions in Bitcoin (BTC). Bitcoin is a new form of decentralized, electronic currency. It's characteristics mean that it can be extremely hard to track Bitcoin owners and users, if sufficiently adept at maintaining operational security. Some members of NovAnoN appear to have a high degree of sophistication with Bitcoin's capabilities, and knowledge of global financial systems, which may allow them to extract illicit funds from Bitcoin into more fungible assets. One or two may have advanced degrees in economics or business.

Recent conversations between these individuals speculated on how to manipulate the price of Bitcoin using coordinated Ransomware attacks and other techniques. Hospital ransomware attacks of 17 May, 2017 corresponded with a four per cent increase in the price of Bitcoin. Whether or not NovAnoN carried out this attack, it is clear they were watching the effects and will learn from the example. It's not yet clear how NovAnoN plans to extract value from such a short-term fluctuation, but they may experiment with several approaches, then increase frequency and scale once they have a working method.

Jurisdictional Challenges

As with many virtual networks and trans-national social movements, NovAnoN appear to spread around the world. There does appear to be a disproportionately high concentration in mainland Europe, which may be a result of high unemployment in some areas, tradition of anarchist and anti-globalist sentiments and high levels of education. Responding to the threat, therefore, will also be highly challenging. In addition to

the sophisticated, centralized cell structure and de-centralized, compartmentalized action, each cell is likely spread across multiple national jurisdictions. This complicates both the identification and linking of specific individual activities, but also coordination of the response.

Assessed Risks

NovAnon represents a new type of hybrid threat. Its members have learned important lessons from previous groups and have evolved their model to mitigate previous weaknesses. The mix of ideological and criminal motivations with virtual and real-world action makes their future actions unpredictable. If able to synchronize their various capabilities, they could achieve a disruptive event of significant magnitude.

Classified by: Direction générale de la sécurité intérieure
Reason: 1.5(c)
Declassify on: 25X

Cyber 9/12 Student Challenge

Intelligence Report III

INSTRUCTIONS

Your team will take on the role of experienced cyber policy experts who were invited to brief a task force of European leaders (including heads of state, heads of government, ministers of defense and foreign affairs, directors of intelligence services, and representatives from the private sector) called to address an evolving cyber crisis. This packet contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure and services in Europe. The attacks notionally take place in spring and summer 2018. The scenario presents a fictional account of political developments and public and private reporting surrounding the cyber incident.

You need to provide information on the full range of policy response alternatives available to respond to this crisis, and your team has been tasked with developing four policy recommendations to pass on to the task force. You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform one task:

6. **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy options and recommending one to the task force.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Don't fight the scenario.* Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- *Think multi-dimensionally*. When analyzing the scenario, remember to consider implications for other organizations and domains (e.g., private sector, military, law enforcement,

information operations, diplomatic, etc.) and incorporate these insights along with cybersecurity.

- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: **Office of the High Representative of the EU for Foreign Affairs and Security Policy**
Re: **Cyber and Kinetic Attacks in Istanbul**
Sent: **Thursday, June 21, 2018 6:20 PM**

The date is June 21, 2018, and since you last presented your policy recommendations to the European task force, we have witnessed a major cyber incident posing an imminent threat to Europe and neighboring regions. Given the urgency of the situation, the chairman of the task force has asked your team to consider the latest information available and develop additional policy response options to present at the next task force meeting in 15 minutes.

To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action.

When generating each of your **four** policy response alternatives, the task force requests that you consider the following potentially conflicting interests both at the national level and EU and NATO levels. These are provided as suggested starting points and are not meant to limit your policy responses.

- **What should be the highest priority when responding?**
- **Is this incident merely a crime? Is it the first stage of an attack? Is it war?**

Additionally, this document is accompanied by the following documents that may assist your team in preparing its policy response alternative recommendations:

- **Tab 1 –** Flash Intelligence Bulletin to NATO Members, NIFC
- **Tab 2 –** Tweets using #NATOSummit from the verified accounts of
    - NATO Source - a NATO dedicated information service
    - Robbie Gramer - a journalist at Foreign Policy Magazine
    - Reuters
    - The Turkish Health Ministry
    - NovAnoN
    - NATO Ambassador Sorin Ducaru

Tab 1: Flash Intelligence Bulletin to NATO Members, NIFC

INTELLIGENCE FUSION CENTER
NORTH ATLANTIC TREATY ORGANIZATION

NATO's Intelligence Fusion Center is issuing this bulletin to help facilitate the sharing and fusion of intelligence related to the Istanbul attacks and the continuing ransomware attacks in Europe, as well as to support the planning and execution of humanitarian and security operations in affected regions.

June 21, 2018 6:12 p.m.

Explosions near NATO Summit Security Perimeter in Central Istanbul; Ransomware Affecting Patient Care in Area Hospitals

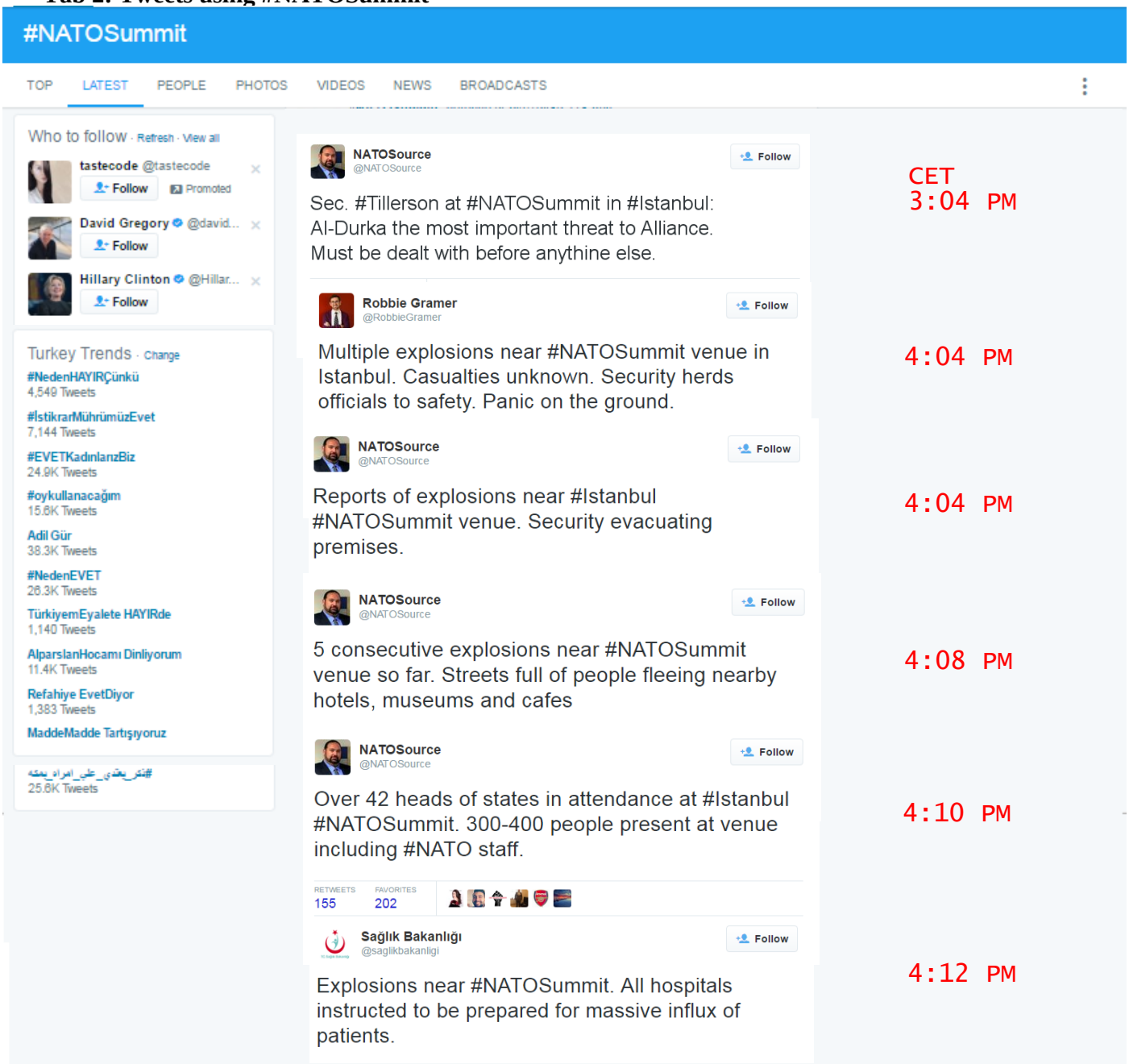
- Multiple, coordinated explosions occurred next to three security checkpoints at the NATO Summit Security Perimeter between 4:02 p.m. and 4:10 p.m. CET (5:02 p.m. TRT).
- Istanbul police has confirmed at least 41 fatalities; hundreds wounded, many with life-threatening injuries caused by the explosives and a stampede at one of the security check points.
- Turkish Ministry of Health (Sağlık Bakanlığı) reports that at 4:40 p.m. CET, the two largest area hospitals – the only two designated Lever 1 trauma centers - began experiencing outages of medical devices and workstations resulting from ransomware.
- Patient care in hospitals remains severely disrupted, as devices and patient records are unavailable, and the death toll is expected to rise.
- NATO Supreme Headquarters Allied Powers Europe (SHAPE) Joint Medical Division has deployed all its 20 doctors present at the Summit to the affected hospitals.

- Open source intelligence collected by NIFC officers indicates that NovAnoN has claimed responsibility for the kinetic and cyber attacks. NIFC believes this claim to be credible. Additionally, ransom demands originating from NovAnoN-affiliated social media appear to match Bitcoin addresses associated with the ransomware in Turkish, Belgian, and Dutch hospitals affected.

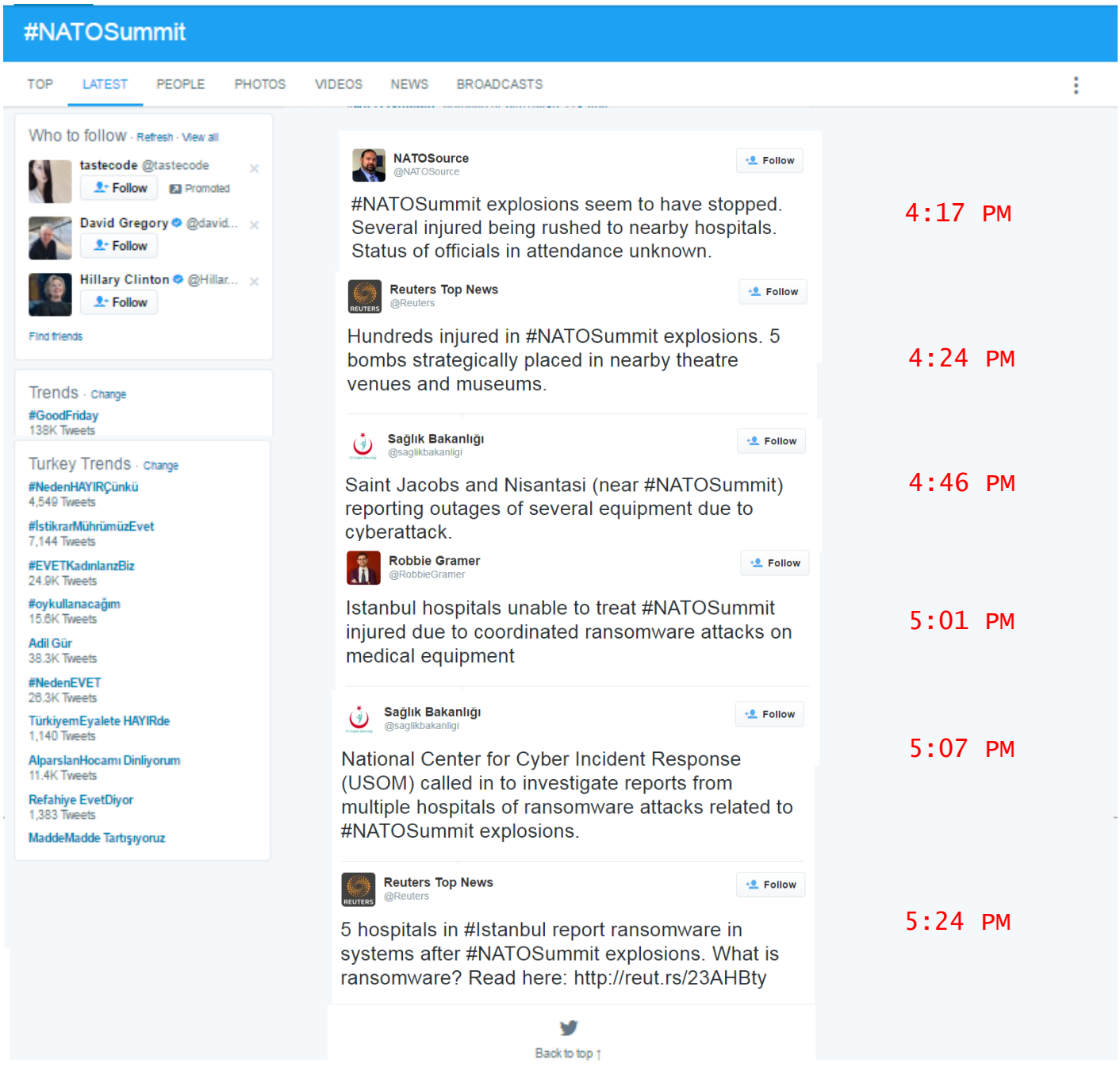
Resurgence of Hospital Ransomware in Brussels and The Hague

- 3 hospitals in Brussels metropolitan area and 2 hospitals in The Hague are under renewed ransomware attacks beginning at 5:45 p.m. CET.
- The attacks are severely affecting patient care, with new patients being turned away and admitted patients evacuated to nearby hospitals.
- Links between the attacks in Istanbul, Brussels, The Hague, and earlier attacks against 28 healthcare facilities across Europe are under ongoing NIFC investigation.
- News of the attacks is spreading quickly on social media, and sentiment analysis in Brussels indicates fear and stress are as high as those measured after the 2016 terrorist attacks in the city.

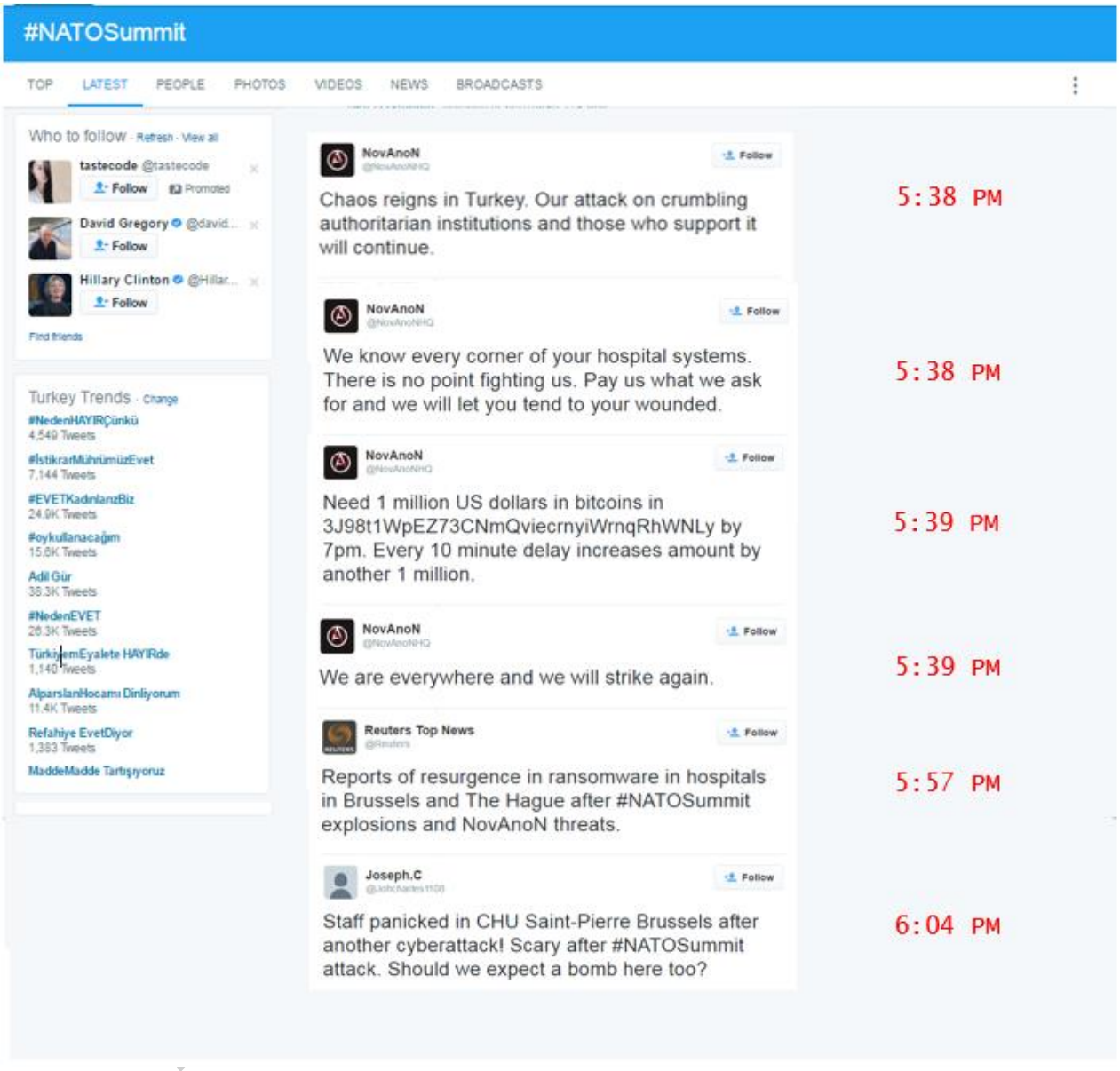
Tab 2: Tweets using #NATOSummit



Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

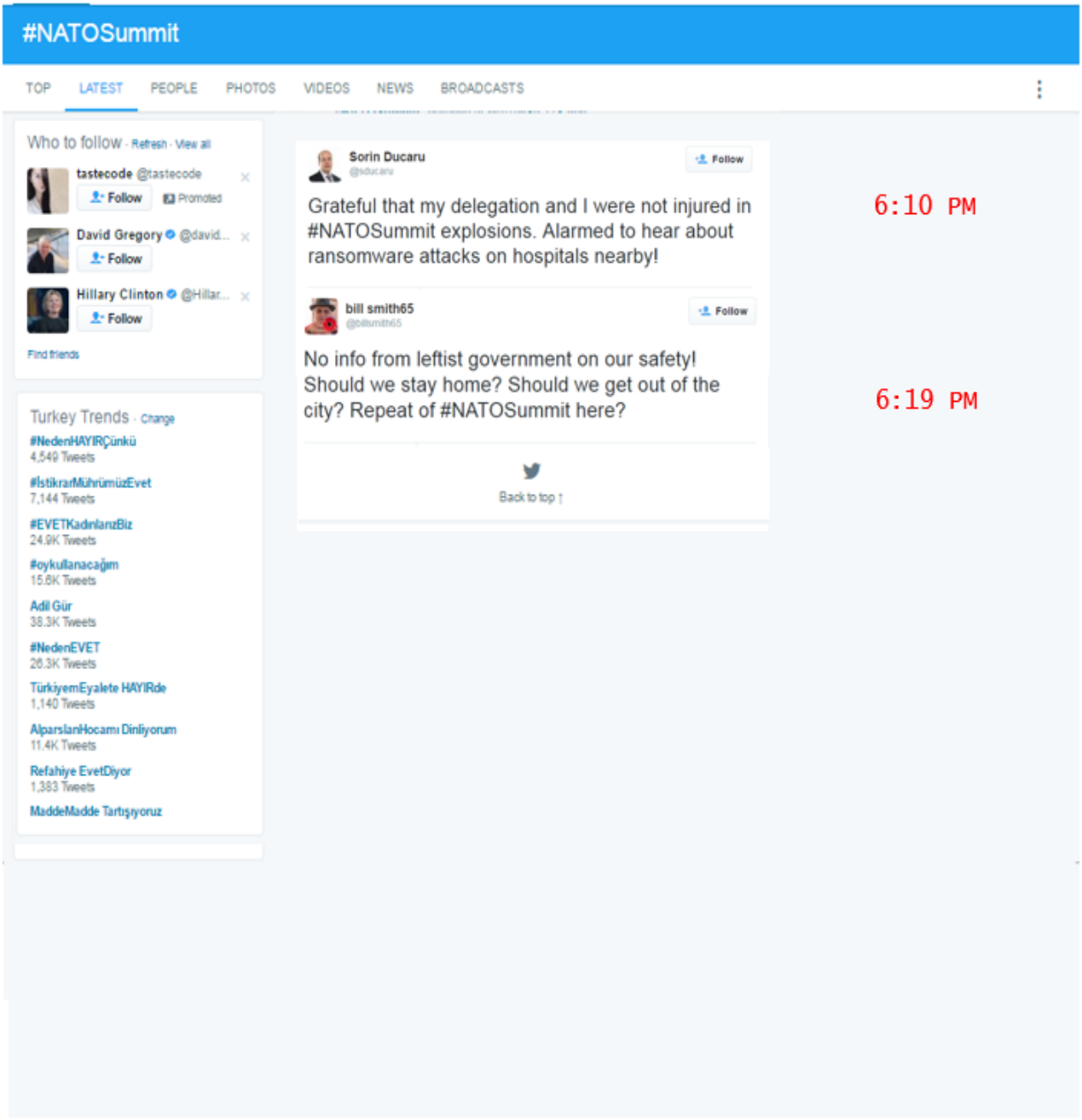


Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.



Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.



Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.