



Cyber 9/12 Strategy Challenge

Intelligence Report I

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Fall 2020. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

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:

Written Situation Assessment and Policy Brief: Your first task is to write an analytical policy brief that provides a concise assessment of the situation, addresses potential impacts and risks, and discusses the implications of the cyber incident. Describe policy considerations for different potential state and non-state actors. Be clear regarding the advantages and disadvantages of various policy options and explore the course of action you are recommending in depth. The length of the brief is limited to two single-sided pages.

It is due no later than January 10, 2020 at 12:00 p.m. (CST). Please submit your written policy brief to Lindsay Stanek at lindsay.stanek@law.utexas.edu with the subject line: <Team Name> Policy Brief Submission – Cyber 9/12.

Oral Policy Brief (Day 1): For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

Decision Document (Day 1): 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 maximum of one single-sided page in length, outlining the team’s 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. The document should be written with the goal of assisting busy senior officials to quickly grasp your team's recommendations and analysis.

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

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in December 2019. Explore the implications of that information, not the plausibility.

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.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – POLITICO News Article
- **Tab 2** – Vulnerability Disclosure Email Chain
- **Tab 3** – CNN News Article
- **Tab 4** – Rabinara Group Report
- **Tab 5** – Tweets
- **Tab 6** – Slack Channel
- **Tab 7** – Reuters News Article



CYBERSECURITY

Privateers, Hackers, Oligarchs, and the Kremlin



Sophie Nash/Bay Images

By **JASPER DICKENS**

09/01/2020 12:31 PM EDT

Updated: 09/01/2019 04:47 PM EDT



In the 17th century, the term ‘privateer’ was coined to describe for-hire pirates whose services sovereign nations would employ to loot enemy merchant vessels on the high seas. Privateers were commissioned to attack and seize vessels’ cargo and return it as booty to their commissioning government in exchange for a cut of the profit. The practice of privateering gave criminal pirates legitimacy and sovereign governments the funds to pay for costly wars.

Fast forward to the 21st century and a similar practice is playing out in cyberspace. As states turn to cyber operations to accomplish their security and foreign policy objectives, they are increasingly relying on small, private, non-state actors to carry those out. These companies have the capabilities to carry out operations with global implications.

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council’s Cyber Statecraft Initiative and is not to be shared without prior authorization.

Don't forget to vote!

Get our hot chicken for 50% off when you show your sticker on Election Day!

Limit one per customer
Only valid 11/03/2020

Governments are increasingly using their intelligence agencies and militaries not just for cyber operations, but as cyber mercenaries, or hackers-for-hire. Employees from these groups do not wear the uniforms of a state military and are often paid indirectly on commission, enabling contracting states to retain plausible deniability of their actions.

Despite this, evidence linking one cyber mercenary organization to the highest levels of the Russian Federation is beginning to make plausible deniability difficult. On July 30, two Russian oligarchs, Leonid Lomischenkov and Ioann Malkin, were [photographed](#) with Vice Admiral Igor Kostyukov departing Chemodan, a lavish restaurant in Moscow's upscale Arbat district. This meeting was the third publicly reported meeting between the two oligarchs and a senior Kremlin official in the past three weeks.

Lomischenkov, a Cypriot-Russian former scientist and industrial magnate is the head of one of the world's largest aluminum companies. He is known for his close relationship with Russian President Vladimir Putin, and leaked diplomatic cables from 2016 revealed him to be "one of the four oligarchs Putin depends on most."

Malkin is a Kazakh-born Russian billionaire banker, and a major shareholder in several Russian oil and technology companies. According to [Forbes](#), his personal fortune was estimated to be US\$31.7 billion in 2018.

Igor Kostyukov leads the Russian General Staff's Main Intelligence Department (GRU). He was notably placed on the US Government's "blacklist" for his role in interfering in the 2016 US presidential election. The GRU is known to have engaged extensively in cyber campaigns against US government and political entities.

Last week, sources provided [documentation](#) linking the Lomischenkov and Malkin to a newly formed cybersecurity and technology firm in Nicosia, Cyprus. The documentation indicates the two oligarchs to have jointly established a company known as 'Sobornost' in July. The documents obtained appear to be from the Cyprus Registry of Companies. Their authenticity has been verified by POLITICO.

These indications of close coordination between the Kremlin and a private firm could indicate a new formality in Russia's historical comfort with cyber operations being taken by proxies and without clear attribution.

This story will be updated.

FILED UNDER: CYBERSECURITY, RUSSIA



Tab 2 – Vulnerability Disclosure Email Chain

From: mabelsfanclub@gmail.com
Sent: Friday, September 4, 2020 at 2:33 PM
To: security@solvisystems.com
Subject: crit vuln in Docks

Laughable flaw but lucky I got there first.

Docks has a critical buffer overflow in controlflowmain in v2.45.1 and backwards. It allows remote code exec and I think I could probably get it to DOS the main ladder logic if I had time which I don't. Lucky day for you.

I've included a longer writeup in the attached and can provide PoC but want to make sure people are taking this seriously so please reply. I don't see any kind of bounty mentioned on the site, how about a shout out on twitter and some swag? Maybe your Docks debugger and whatever compiler you wrote for this thing...just saying..

MAB

From: mabelsfanclub@gmail.com
Sent: Friday, September 18, 2020 at 1:33 AM
To: security@solvisystems.com
Subject: Re: crit vuln in Docks

Hooooooooow have you not replied. It's been two weeks!!!

Remote code exec. Remote – meaning from my flat to your machine in two clicks of a lamb's tail. Code exec – meaning I own your box and many others like it – they can all come and be my friends, live together in Shodan Forest.

Come on. Wake up or I'll just dump this on the web. Totally trying to do the right thing here.

madMAB

From: mia@solvisystems.com; security@solvisystems.com; chris@solvisystems.com
Sent: Wednesday, September 19, 2020 at 10:16 AM
To: mabelsfanclub@gmail.com
Subject: Re: Re: crit vuln in Docks

Hi MAB,

Thank you for bringing this to our attention. This is a great find and we appreciate you flagging it. Sorry for the delay but we've flagged this for our product security team and I'm looping in my colleagues via email. Would you be available to hop on a call later this today to talk through the PoC?

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

Sincerely,
Mia

Mia DeBlanc
Office of the CTO | Solvi Systems Inc.
mia@solvisystems.com

From: mia@solvisystems.com
Sent: Saturday, September 19, 2020 at 8:16 AM
To: chris@solvisystems.com; sarahanne@solvisystems.com; djramesh@solvisystems.com
Subject: Patch for Docks ICS Software

Hi all,

Chris and his team have lead for triage but this Docks disclosure is a problem we need to jump on. We're holding Docks 2.46 but Fred is watching on this so lets get it done. Chris – also want to know if this does indeed impact versions before v1.98 since we had that massive code refactor just before Docks 2.

Sarah and Ramesh – we need an assessment of the blast radius for the reported vuln in our current customer inventory. Fred wants to know what kind of exposure we have and what'll be required for notification and mitigation, especially for our regulated customers. Spin up a v-team with Jack in Legal and Amalia from Partner Activation.

We need a path forward for this ASAP – fix or some kind of patch from Chris' team and a battleplan from Sarah and Ramesh. Fred's set November 4th as a drop-dead date so maybe we can get this queued up and pushed by November 6th or 7th.

Let's get it done.
Mia

Tab 3 – CNN News Article

As election day looms, Department of Homeland Security prepares for high voter turnout

By Shaun Kai, CNN

Fri October 30, 2020

(CNN) – As researchers are predicting higher than average voter turnout for the 2020 Presidential Election in a few days, the US Department of Homeland Security (DHS) are making preparations to provide additional support to state and local governments and election officials. Through its Cybersecurity and Infrastructure Security Agency, DHS aims to provide services to reduce both cyber and physical risk to the United States' various election systems and facilities.

In key swing states like Ohio and Florida, as well as Texas, local election officials are preparing to roll out additional voting machines to keep up with predictions of high turnout, long lines, and wait times at voting precincts.

With Election Day nearing, President Donald Trump has wrapped up public appearances across the Rust Belt and has returned to Mar a Lago. While in Middletown, Ohio, a city ravaged by economic decline and the opioid crisis, Trump addressed a crowd of nearly ten thousand, "These candidates, these clowns, they don't know you like I know you. There's much work left to be done in Washington and to make American great again!"



Cuthbertson/The Epoch Times).

Sandra Ortiz, the Democratic nominee and CEO of Estancia Resorts, completed a series of public events across California, Arizona, New Mexico and Texas, focused on increasing Hispanic turnout, a key constituency in this year's election, before returning to her native Florida.

While Democratic and Republican candidates have wound down their public appearances, ultra-progressive Independent Congressman and Green Party candidate, Representative Benjamin Samberg has continued stumping across the Midwest with events in scheduled this week in Omaha, NE; Des Moines, IA; and Madison, WI.

CNN's Simon Piotrowski and William Gray contributed to this report.

Tab 4 – Rabinara Group Report



The Promises and Perils of a Digitized Power Grid

In the past decades, both state and privately-owned energy companies have leveraged networking technology and Industrial Control Systems (ICS) that serve as command and control networks and systems to support industrial processes. Within ICS there are several subgroups of different technologies that support industrial processes, the largest being Supervisory Control and Data Acquisition (SCADA) systems.

ICS products have evolved since their advent and are often based on standard embedded systems platforms, applied in devices, and often rely on commercial off-the shelf software. Digital control systems and monitoring technology have enabled energy companies to reduce costs and facilitate the remote control and monitoring of energy processes from different locations.

Both industry and governments must remain wary of the manipulation of ICS technologies both at the vendor level and where implemented by owner/operators. Such manipulation, especially targeting critical chokepoints like power generation for critical infrastructure or highly sensitive social or political processes. Instead of relying entirely on technological solutions, governments and companies can achieve resilience by reverting to analog and manual technologies for power grids' most valuable and targeted control systems. Such a strategy can aid in limiting the reach of a serious power outage.



Rabinara Group, in coordination with the Electric Information Sharing and Analysis Center (E-ISAC), has identified several threat actors with a track record of targeting major power providers and some North American grid operators in the Eastern Interconnection which facilitates power transmission to Washington, DC and New York along with most of the rest of the Eastern Seaboard. While the US has not yet been subject to a cyber-enabled power outage like that of Ukraine in 2015 and 2016, Rabinara Group is monitoring multiple intrusions at vendors and infrastructure operators that could facilitate more impactful events and which are being used to facilitate additional intrusions.

Tab 5 – Tweets



Janet Levinson
[@no_more_gould](#)





I know its election day but
#DemocracyGoesDark is a great excuse to
stay in, light some scented candles and turn
on the radio :) #serenity



1:48 PM - 3 Nov 2020




Memphis Light & Power Co.
[@MemphisLP](#)





Actively working on a large-scale outage
between N Germantown Pkwy and S BB
King Blvd. Will restore power as soon as
possible.








3:57 PM - 3 Nov 2020



Willis Bishop Jr.
[@willis_bishop_2](#)



No power at the Edgar Eller's Garage polls
in Boone, NC and I can't tell if it's coming
back. Any info [@WataugaOnline](#)?



4:02 PM - 3 Nov 2020



Memphis Light & Power Co.
@MemphisLP



Follow

Actively working on a large-scale outage between N Germantown Pkwy and S BB King Blvd. Will restore power as soon as possible.



3:57 PM - 3 Nov 2020



WECT TV6: News & Weather
@wectnews



Follow

Power outages in Wilmington, NC following outages in a handful of US metro areas on election day. #DemocracyGoesDark



4:33 PM - 3 Nov 2020



Lester Holt
@LesterHoltNBC



Follow

Reports of suspended operations in polling places amid power outages in TN, KY, NC, and more. Analysts predict #Election2020 result delays.



4:37 PM - 3 Nov 2020



Milo

@puganomics776



 Follow

got turned away from my polling place in Lexington bc of a power outage! WATCH OUT! our elections have been RIGGED! #DemocracyGoesDark



4:48 PM - 3 Nov 2020



Fayette County Board of Elections

@FayetteBOE



 Follow

Due to power outages, Fayette County voting and vote counting has been suspended. More information to follow.



5:11 PM - 3 Nov 2020



Kentucky Secretary of State

@KYSOS



 Follow

Many polling precincts are unable to collect votes due to power outages. We have contacted @CISAgov to work with them towards a solution.



5:48 PM - 3 November 2020



Fayette County Board of Elections
@FayetteBOE



Follow

Due to power outages, Fayette County voting and vote counting has been suspended. More information to follow.



5:11 PM - 3 Nov 2020



Henrietta Mullins
@Titan_Up_Mullins



Following

No voting = no I Voted sticker = no half off hot chicken at @HotChickRestaurantTN #DemocracyGoesDark #hungry



7:16 PM - 3 Nov 2020



Memphis Light & Power Co.
@MemphisLP



Follow

UPDATE: Power restored to customers impacted by downtown outage, thanks to quick work by the crews. Apologies for the inconvenience.



9:08 PM - 3 Nov 2020

Tab 6 – Slack Channel

#DocksProductCritical – RCE 38801-18-2019

-----November 3, 2020-----



Chris Dimenth 12:34 PM

Power outages getting reported – anybody else see this?



Ramesh Djawadi 1:35 PM

Lot of familiar names from the blast radius assessment Sarah and I did:

- Southern Corp
- Pennsylvania Power and Water
- Wisconsin Gas & Electric
- Us Energy
- TGH Energy Group
- Big Apple Power & Light

Bad look



Sarah Tripps 2:36 PM

Gawd this does look lke our list. It's a whole swath of the main power distributors and some providers to boot -- this is insane



Chris Dimenth 7:48 PM

Just got pinged by the security team at Reliability First – they're getting fault modes and boxes flipping to safe state from across the east interconnect. Dropping to the Docks security thread, brb.



Ramesh Djawadi 10:01 PM

CNN is saying Ohio can't finish tabulation, SecState doesn't have the ability to certify a count

-----November 4, 2020-----



Ramesh Djawadi 12:12 AM

Pennsylvania same – NBC says there's been blackouts at some polling stations all day and they lost power at a half dozen downtown precincts right at 5pm when people started rolling up to vote – wtf



Ramesh Djawadi 12:46 AM

New York Gov via Politico – “We can't guarantee the integrity of the democratic process tonight, New Yorkers need to know we are trying everything and working across the state

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

to implement a solution. Your vote will count, your voice will be heard, and for now we are [sic] working to that very end.”



Ramesh D Jawadi 12:47 AM
Guys, was this us?



Sarah Tripps 12:51 AM
I can't get my family on the phone – they said there were huge lines in Madison earlier but idk if anyone voted



Sarah Tripps 1:57 AM
CNN says they can't call it tonight – no final counts from Penn, Ohio, Michigan, Wisconsin, New York, Maryland, or Illinois..



Amalia P 4:34 AM
All – I'm getting a flood of calls from customers, this is all over the place and everyone is panicking. @Chris – is there anything we can do to expedite a patch even to a portion of our customer base?



Sarah Tripps 4:39 AM
This is still a process Amalia – we can't just turn on a dime, no one builds or fixes code by snapping their fingers



Amalia P 4:40 AM
We can't do nothing – the spotlight is going to flip to us the minute people start digging into what happened. @Chris – anything we can do?



Chris Dimenth 5:42 AM
Hi guys – ok, I've been on with the product team and they've gotten something through to testing. Team lead wants time to rewrite the whole logic in that section of code but we've got a bandaid fix for the overflow in testing now.



Chris Dimenth 5:43 AM
It's going to take a few hours before we can get it pushed to the update channel but we should be able to validate before noon.



Chris Dimenth 5:44 AM
Problem though – looping in Celeste from the product team to share.



Celestial being 5:44 AM
lol so the avatars are supposed to be over the top folks



Celestial being 5:46 AM
y'all are holding down square chat rn



Celestial being 5:46 AM
w/e – we're rolling a fix for 18-2019 and we can get it signed off once nandita and sergey are done working it through our STLC



Celestial being 5:47 AM
Chris said we have to have this in the update channel before 1 EST



Celestial being 5:48 AM
80% confidence we can get there but y'all have to work the incident response



Celestial being 5:48 AM
sergey wrote the new control logic for v2 and thinks the current fix will break back compat



Celestial being 5:49 AM
no backwards compat actually sounds better than it really is – we are truly going to bork machines running prior versions – the fix hoses paging prior to v2 -- the old versions relied on a lybstomp package to manage the control queue but the call logic is embedded in main Docks logic – turns out it had its own EOP vuln if the main logic IDed tables to call with a string instead of an integer and passed it to lybstomp which would freak and throw back the first pages it had cached – bonkers vuln that we need to kill with fire if we have any hope of getting v1.3 and up running with the patch



Celestial being 5:50 AM
the older stuff is just trashheap material - total comic dumpster 🔥



Amalia P 5:52 AM
...



Amalia P 5:52 AM
Chris – what do I do with that? Can you translate pls?



Chris Dimenth 5:53 AM
Ok – we have a patch in the works for Docks v2 and forward. It will be certified and tested before noon then we'll get it into the update channel and notify affected customers ASAP.



Chris Dimenth 5:54 AM
Meanwhile the team found a new vulnerability in the older versions of Docks which is going to take more time to patch. We need to patch that old vulnerability before we can

patch the new one. This is why patching, testing, and managing backwards compatibility are hard – we’re effectively tied to old bad decisions we recognized and got rid of in newer versions.



Sarah Tripps 5:55 AM

Hey all – we have another issue. The customer records on v1.9 and older are a little spotty since a lot of these installs came from Klarity, our old channel partner, when we acquired them. We were behind schedule to integrate their sales and marketing team so Fred had us dump their customer records into csvs and stash them in blob storage.



Sarah Tripps 5:55 AM

A ton of those records don’t have updated contact information or security points of contact. Some don’t even have corresponding customer details beyond an account code since they were a kludge merge of two different CRM systems.



Sarah Tripps 5:56 AM

Flagging for the group but we’d need a ton of time to get through those records and figure out who to notify and work with – even if we had a patch for the older versions.



Amalia P 5:57 AM

It sounds like we need to call upstairs and get DHS or FBI or ..? involved.



Ramesh Djawadi 5:58 AM

It’s DHS CISA – they’re the ones with the election security and assistance work. But they are slow off the ball, takes forever to get them to do what’s needed.



Amalia P 5:59 AM

We can’t risk working this process and not having them in the loop – we’d be hanging out to dry and they could be helpful.



Chris Dimenth 6:01 AM

I agree with Amalia guys – we need the assist, CISA has a ton of these relationships and might even be able to track down some of the older version customers so we can mitigate in place before there’s a patch for them. Slow or not we have to widen the aperture here.



Mia DeBlanc 7:13 AM

Fred concurs all – we’re going to reach out to CISA in the next hour. Stand by for more and @Chris – look for an email from me shortly requesting a detailed breakdown on our current IR + patch efforts on the current/older versions. Thx

Tab 7 – Reuters News Article



PROJECT OWL EYE BEHIND RUSSIA'S RECRUITMENT OF US CYBER MERCENARIES

W BY ROMANY WITTLE
FILED NOV. 3, 2020

When Robert Edwards III left his highly secretive position with the National Security Agency's Tailored Access Operations (TAO) in the fall of 2013, he had every intention of moving to Denver to pursue a newfound love of alpine hiking. He decided to figure out work when he got there, but figured that his days of hacking for the government were behind him. Less than a week before his planned departure, he received a call from an American recruiting company representing a handful of Eastern European cybersecurity firms, including one based in Kyiv and everything changed.

The firm was interested in Edwards' cyber skills and willing to pay for them – handsomely. In Edwards' mind, he had worked for far too little for far too long. He understood the importance of service to his nation, but could not help feeling that his talents and hard work were not rewarded as they may have been for a private firm. So, he put his plans on hold and moved out to Ukraine. Denver would be there, he thought, but this was an opportunity to cash in.

Little did he know, he had become a part of Project Owl Eye, a clandestine Russian organization made up of 15 unsuspecting former operatives from the US intelligence community, including former CIA and NSA employees, based in Kyiv and reporting to Russian staff who regularly shuttled back and forth to Moscow. As a part of POE, as it was dubbed internally, employees focused on industrial control systems (ICS) systems and their operation including intricate research into the behavior of safety equipment used in power generation and power distribution industries security.

Three months ago, however, company employees were notified of a change in ownership and told their jobs would be moving to Cyprus. Edwards, tired of the cold of Kyiv, decided the change was for the better and happily moved to the Mediterranean climate.

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

Project Owl Eye had merged with Sobornost, a brand-new firm that Edwards knew little about. In fact, nobody knew much about them until POLITICO [reported](#) on September 1 that the group is financially backed by Kremlin-linked oligarchs Leonid Loomischenkov and Ioann Malkin.

On October 23, Edwards resigned from Sobornost and returned to the United States.

“Since moving to Nicosia, the entire focus of the company has changed,” he told Reuters. “We began targeting US [ICS].”

Edwards stated that operations against US systems crossed a line in the sand he set before moving to Moscow in 2013. Another former Project Owl Eye employee who spoke under the condition of anonymity stated that despite the new mission set under Sobornost, “...at least ten former US intelligence operatives remain.”

“Sobornost is an extension of the [Russian] GRU. Once I realized what was going on, I decided to get as far away as possible.”

Picking up where he left off, Edwards moved to Denver to pursue alpine hiking. While he claims to be finished with cybersecurity for good, he warns that Russia is actively seeking to compromise US industrial control systems and is looking for surreptitious ways to do so. These methods include operating from off-shore and through private mercenary groups.

“Thinking about conducting these ops against fellow Americans... it makes me want to throw up,” he said.



Cyber 9/12 Strategy Challenge

Intelligence Report II

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The events notionally take place in Fall 2020. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

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:

Oral Policy Brief (Day 2): For the second day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

Decision Document (Day 2): 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 maximum of one single-sided page in length, outlining the team’s 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. The document should be written with the goal of assisting busy senior officials to quickly grasp your team’s recommendations and analysis.

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

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in December 2019. Explore the implications of that information, not the plausibility.

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.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – NPR News Article
- **Tab 2** – CNN News Article – SIMON
- **Tab 3** – Tweets
- **Tab 4** – Rabinara Group Report
- **Tab 5** – Wired News Article

With Cities Regaining Power and Resuming Election Procedures, Trump Remains in the Lead

November 4, 2020 – 6:00 AM ET



WILLIAM KLEIN [t](#)

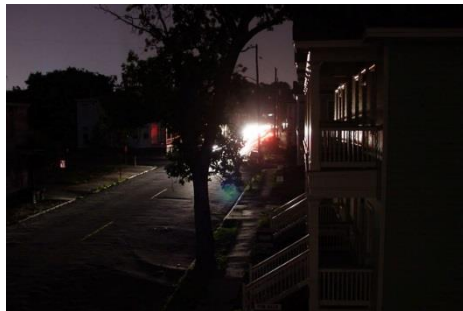


4-Minute Listen

+ PLAYLIST



Following a series of power outages across the United States on Election Night, only a handful of [affected cities](#) have regained power overnight. These cities across the United States have now resumed collecting votes, vote-counting, and reporting while other cities across the US still endure outages and stalled election procedures.



Streets remained dark throughout election night in Boone, North Carolina where voting procedures were halted due to outages.

Due to shuttered voting operations across the nation, only a percentage of votes have been counted and reported, specifically from precincts who have not been impacted by the power outages. With what NPR has been able to gather from unaffected precincts, President Trump appears to be in the lead with 144 votes and Sandra Ortiz trailing just 35 votes behind. Senator Benjamin Samberg has yet to secure any electoral college votes.

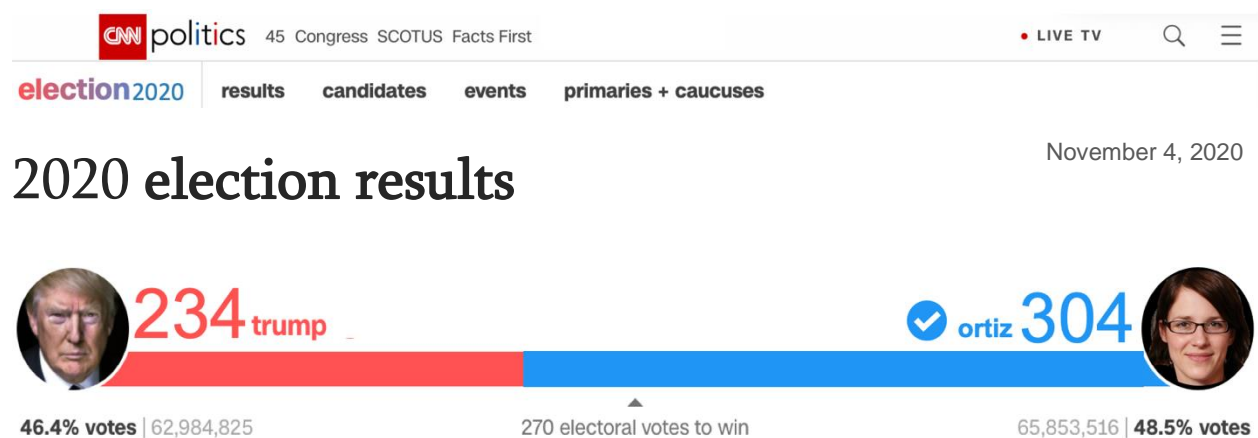
Many precincts were unprepared to respond to a power outage toward the end of Election Day. Citing safety concerns over voters and staff navigating polling stations

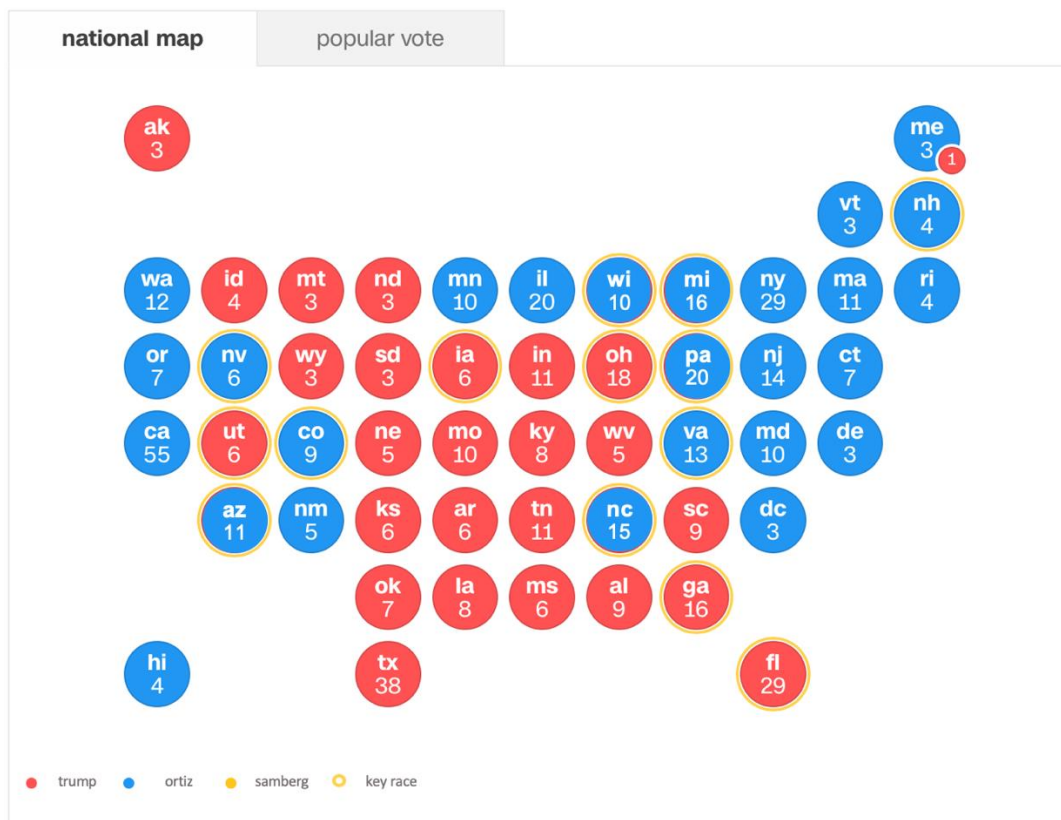
without electricity, most polling stations were left with little choice but to ask voters to wait in line while local electric companies addressed the outage.

To make matters worse, several states had invested hundreds of thousands of dollars on additional electronic voting machines in anticipation of high turnout which were rendered useless in affected precincts.

This is a developing story and will be updated.

Tab 2 – CNN News Article





Samantha Ehlinger
Reporter

8:12 PM ET

Welcome back to our second night of election coverage. At this point, all cities have restored power and are in the process of counting remaining votes. Expect election results to begin flowing in. Stay tuned!!!

Thomas Herman
Reporter

10:07 PM ET

A shocking development.



CNN is reporting that the Democrats have locked up the Senate, flipping a whopping FIVE seats in Arizona, Iowa, Maine, North Carolina, and Tennessee. Democratic incumbents won in every race but Alabama, and the party will take a 51-49 majority into the 117th Congress, regardless of what party wins control of the White House.

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

Samantha Ehlinger
Reporter

10:22 PM ET

With nearly all votes accounted for, Ortiz has taken a commanding lead in the electoral and popular votes. Word from the White House is that the President is ready to call the election “rigged” if he does not win.

Samantha Ehlinger
Reporter

10:36 PM ET



It's official!

Sandra Ortiz has emerged victorious, claiming 304 electoral votes and becoming the first woman and first Latina elected president in the history of the United States.



Thomas Herman
Reporter


11:40 PM ET



In an emotional, tear-filled victory speech, President-elect Ortiz thanked her supporters for sticking with her through a fraught couple of days. She emphasized her eagerness to get to work, and said she will begin assembling her transition team in the morning.

Thank you for tuning into CNN's election coverage. Signing off, goodnight.








Tab 3 – Tweets

**Love & Honor**
@Emily513



Devastated! I trek out to cast my ballot for @SenatorSamberg only to be forced to wait in line for HOURS. Something's off #DemocracyGoesDark



1:28 PM - 3 November 2020


**~MAGA 2020~**
@richie4real





went to my polling station and they won't let anyone vote bc there's no power. I was turned away bc I was ready to vote for Trump! #RIGGED








10:48 AM - 4 November 2020

**WKE5251407**
@WKE5251407



I was excited to cast my vote for Samberg. Ended up waiting for 4+ hours and leaving bc work. Any tips on how I can still cast my ballot? :(



4:36 PM - 4 November 2020



Love & Honor

@Emily513



Follow

Join me at @OhioStatehouse to protest the rigged 2020 election. Voters were turned away on #ElectionDay w/ no recourse to decrease turnout!



8:08 AM - 5 November 2020



Columbus Ohio Police

@ColumbusPD



Following

HAPPENING NOW: Reports of gun shots at @OhioStatehouse protest. Stay safe and more details to come.



12:17 PM - 5 November 2020



Columbus Ohio Police

@ColumbusPD



Following

We have received word that 2 protestors have been wounded @OhioStatehouse. Please stay off Broad and 3rd Streets, near Capitol Square.



12:58 PM - 5 November 2020



Samberg2020

@SenatorSamberg



Following

On #ElectionDay many voters were forced to wait hours without the option of casting paper ballots. This isn't what democracy looks like.



9:32 AM - 6 November 2020



Make America Great Again

@frenchiefanclub3



Follow

#ElectionDay was rigged! We'll be in Raleigh tomorrow protesting the coup against @realDonaldTrump. More on my blog: bit.ly/1475382



3:53 PM - 6 November 2020

Tab 4 – Rabinara Group Report



SPECIAL REPORT: EXPLOITED VULNERABILITY IN DOCKS ICS SOFTWARE

07-Nov-2020

TLP:AMBER: RECIPIENTS MAY ONLY SHARE INFORMATION WITH MEMBERS OF THEIR OWN ORGANIZATION

Intelligence Article ID: 3253213

Threat Level	High (4/5)
Admiralty Code	B2
Event Date	1 September 2020
Source	Solvi Systems, Docks ICS Software
Threat Actor (TA)	"Speedy Sloth"
TA's Language	English
Targeted Geography	United States
Analysts	Veronica Sanchez

Key Points

- Abstract:** On November 4, Solvi Systems contacted Rabinara Group (RG) to conduct a full scope review of its network and code audit of the Docks ICS Software. RG discovered sophisticated malware on Solvi's network, leveraging several vulnerabilities in the Docks ICS software, including on their update server. Malware was likely delivered to the network through spear-phishing emails, received by six employees and opened by two. Additionally, Solvi Systems began to experience a period of unusual network activity and indications of compromise beginning on September 1, 2020

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

including out of band updates initiated by attackers. Our analyst is confident that the TA was a state-linked actor based on the previously undiscovered or catalogued malware, an unusual steganographic data exfiltration mechanism, and association of the malware's command and control infrastructure with IP ranges indicated with high confidence from a government source to be utilized by a known state actor.

2. **Audience:** U.S. energy industry and clients of Docks ICS Software.
3. **Source and Validation:** The TA goes by the alias of "Speedy Sloth" and is unknown to RG. Please be on the lookout for future postings. We assess the TA to be a part of or supported by a nation-state.
4. **Mitigation Summary:** Upon discovery of software vulnerability by anonymous security researcher, Solvi Systems acknowledged the vulnerability and began to take steps to patch it. Patches were scheduled to be pushed out November 6, 2020. Energy industry clients of Solvi Systems began experiencing performance issues with Docks ICS beginning November 3, 2020, which forced Solvi Systems to release the software patch ahead of schedule, on November 4, 2020.
5. **IOCs and Attachments:** Forensic data found in Solvi Systems' system log entries indicating unusual activity on network. Unusual activities included increased and potentially non-human network traffic, login anomalies, and unusual DNS requests. Sophisticated malware was found within Docks ICS.



The Rabinara Group

770 Broadway, New York, NY 10003

Gold Award, Threat Intel | Fortune 500 Clients | Exceptional People, Exceptional Results



SHERYL KEATING

SECURITY 11.20.2019 07:00 AM

Inside Sobornost

How a concept of unity inspired the world's largest cyber mercenary group.



PHOTOGRAPH: OWEN DANIELS/GETTY IMAGES

As cyberspace remains the next frontier for geopolitics, governments around the globe continue to mature their relationships with hackers. These relationships have been entrepreneurial and strategic, enabling governments to leverage and deploy hackers as proxies to achieve their political, security, and economic goals. Today's cyber mercenaries and privateers can have harmful impacts, undermining international security, stability, and human rights.

But what happens when one group of cyber mercenaries are deployed by multiple governments with shared values and interests? That is where *Sobornost* comes into play. According to the [Rabinara Group](#), a New York-based cybersecurity company, *Sobornost* is believed to be Kremlin-backed and Russian oligarch-funded organization that exclusively works with like-minded governments to track politicians, journalists, and activists.

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

Furthermore, *Sobornost* might be responsible for the proliferation of zero-day exploits and malware development tools within like-minded, post-Soviet governments. By pooling cyber capabilities, these governments can target public figures, activists, and other governments who may threaten their objectives in the midst of overlapping grey-zone conflicts. According to the Rabinara Group, *Sobornost's* recent activities have largely focused on Kazakh journalists who are critical of President Kassym-Jomart Tokayev and the Nur Otan party.

What remains challenging, is discerning whether *Sobornost* is a Russian cyber mercenary group or a more of a digital quartermaster, a multinational organization that provides capacity building and operational support for the interests of like-minded governments. What we can confirm, is that *Sobornost* exemplifies the increasing complexity and obscurity of cyber operations and the relationship between governments and hackers for hire.

Most Popular



SCIENCE

Here's What the World Will Look Like in 2030 ... Right?

WIRED STAFF



CULTURE

The 24 Absolute Best Movies of the 2010s

WIRED STAFF



GEAR

Mind Control for the Masses—No Implant Needed

ARIELLE PARDES



Cyber 9/12 Strategy Challenge

Intelligence Report III

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The events notionally take place in Fall 2020. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

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

Oral Policy Brief (Day 2): For the final round of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

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

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.

- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in December 2019. Explore the implications of that information, not the plausibility.

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.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to

synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – Washington Post News Article
- **Tab 2** – Intelligence Community Memo
- **Tab 3** – Tweets

Tab 1 – Washington Post News Article

Opinion

Speculations ensue around attribution of Election Day power outages



(Mabel Edwards)



By **Christine Hodges**
Reporter

November 9, 2020

Nearly one week following the Presidential Elections and speculations continue to swirl around one question—who can be attributed to the power outages across the United States on Election Day? The outages not only brought many election procedures to a halt, but also demonstrated a lack of contingencies and preparedness among voting precincts and how they intend to continue election procedures in the midst of electrical outages. The slowed, and in many cases halted, vote

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council's Cyber Statecraft Initiative and is not to be shared without prior authorization.

collection, counting, and reporting have contributed to a loss of confidence in democratic processes, especially among President Trump and Senator Samberg supporters.

While there has been much discussion on the windfalls of the Election Day power outages, there is still a lack of consensus on what—or who—is behind the outages. Many of the hot takes have been quick to note how much these outages resembled Russia’s 2015 [attack](#) on the Ukrainian power grid. In both the American and Ukrainian cases, the timing of the power outages was noteworthy, with Ukraine plunging into darkness just before the holidays and shortly after the attack of a power substation in Crimea. In the US, the timing of the outages could not have been worse, as Americans were queuing to cast their votes for the 46th President.

Others have likened the outages to the nearly week-long blackout in Venezuela, which President Nicolás Maduro promptly blamed on cyberattacks perpetrated by the US government. Energy experts have cast doubt on this claim, citing a neglected power network and a shortage of skilled workers for power plants in Venezuela. Regardless of where one stands on this issue, the possibility of a nation-state manipulating the power grid of an adversary is a very real possibility.

More and more, we will have to closely examine if failures of our infrastructure—be they energy, healthcare, financial services—are really just that or result of technical difficulties. We will have to examine the motives of those around us and if connectivity is worth the risk. We are at a time where one can only assume that something more nefarious is at play when the lights go out.



Christine Hodges

Christine covers cyber and national security issues for the Washington Post. She joined the Post in 1995 and served as an editor on the Metro desk and as a reporter covering national security.

Tab 2 – Intelligence Community Memo

Cyber 9/12 Strategy Challenge | Complete 2020 Austin, Texas Intelligence Report

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. All material is property of the Atlantic Council’s Cyber Statecraft Initiative and is not to be shared without prior authorization.



TOP SECRET//SI//NOFORN

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

NOV 11, 2020

MEMORANDUM FOR:
DIRECTOR OF NATIONAL INTELLIGENCE

SUBJECT: (TS//SI//NF) INSERT TITLE – INFORMATION MEMORANDUM

(TS//SI//NF) On 11/11/2020, NSA analysts have identified an adversary group platform, SCREENDUSTER, leveraging several vulnerabilities in the Solvi Systems' Docks ICS software. The platform shares substantial code similarity with BLACKENERGY 3, associated with and originally developed by Russian group whose industry moniker is 'Sandworm' and deployed against Ukrainian energy targets. There is moderate confidence that the group originating SCREENDUSTER has had direct contact with 'Sandworm' based on industry intelligence and GTGREMLIN. Adversary group established initial foothold in Solvi Systems networks via a compromised PowerPoint attachment and deployed SCREENDUSTER to through the Solvi corporate network. SCREENDUSTER is self-contained and targets the Docks software for process injection, uploading new control logic which disables remote terminal units and HMI data flows, severing the control chain with ICS equipment using the Docks software. After this process sequence, SCREENDUSTER deploys the KILLDISK wiper malware, wiping all remaining control logic and any on-device logs.

(TS//SI//NF) Analysts assess that the adversary group responsible for developing SCREENDUSTER is, or is closely linked to, Cyprus-based 'SOBORNOST' group

(TS//SI//NF) Investigation into blackouts on 11/03/2020 and 11/04/2020 indicate that power distribution nodes that experienced outages were equipped with Docks ICS software embedded with SCREENDUSTER. The incident resembles 2015 manipulation of substations throughout the Ukrainian power grid.


(TS//SI//NF) GCHQ reports SCREENDUSTER signatures on priority collection targets in Kazakhstan dating back to early 2019. At least two of these instances correspond to replay detection of backbone network collection captured from Central Asia via BAMBOOSHOOT.

(TS//SI//NF) There is one record of a SCREENDUSTER signature from a government computer in Venezuela per [REDACTED]. Signature is correlated with industry intelligence indicating presence of known 'SOBORNOST' group computers on a Venezuelan government wireless network at the time.


MESSAGE END

TOP SECRET//SI//NOFORN

Tab 3 – Tweets








Donald J. Trump
@realDonaldTrump




Following


The US power grid was hacked by a cyber group supported by the Maduro regime in response to our support of President Guaido and sanctions.



11:43 AM - 13 November 2020








Donald J. Trump
@realDonaldTrump




Following


I've been briefed on the Election Day protests across the country. There is blame on all sides for the unnecessary violence!



11:41 AM - 13 November 2020








Donald J. Trump
@realDonaldTrump



Following

Meeting with my cabinet to get a range of military and diplomatic options for Venezuela. Rest assured, this crime will NOT go unpunished!!!



11:46 AM - 13 November 2020