Published by CCDCOE

WMGIC x NATO ACT Cybersecurity Challenge

K. Floyd, K. Hoving, T. Lawrence, T. Liu, N. Perez, P. Pernik (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

WMGIC

WILLIAM & MARY
CHARTERED 1693

Published by CCDCOE

WMGIC x NATO ACT Cybersecurity Challenge

K. Floyd, K. Hoving, T. Lawrence, T. Liu, N. Perez, P. Pernik (Eds.)

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

WMGIC
GLOBAL INNOVATION CHALLENGE

WILLIAM & MARY
CHARTERED 1693

WMGIC x NATO ACT Cybersecurity Challenge

ISBN (pdf): 978-9916-9565-1-9

COPYRIGHT AND REPRINT PERMISSIONS

NATO CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 34 nations providing a 360-degree look at cyber defence, with expertise in technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual 2.0, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields and hosts the International Conference on Cyber Conflict (CyCon), a unique annual event in Tallinn, joining key experts and decision-makers from the global cyber defence community. As the Department Head for Cyberspace Operations Training and Education, the CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. The Centre is staffed and financed by its member nations: Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

WILLIAM & MARY

William & Mary, in Williamsburg, Virginia, carries on an educational tradition that traces back more than three centuries. As the second-oldest institution of higher education in the United States, William & Mary was founded by King William III and Queen Mary II of England as an American overseas campus representing the British Crown. Known as the alma mater of globally-renowned historical figures such as George Washington, Thomas Jefferson, James Monroe and John Marshall, William & Mary today is a leading force for international education and training ground for international specialists around the world. William & Mary boats more than 40 undergraduate programs and more than 40 graduate and professional degree programs, attracting students from 50 states and more than 60 foreign countries.

The mission of the William & Mary Whole of Government Center of Excellence is to train a new generation of future leaders who have hands-on, practical experience working across the different organisational cultures. These leaders must harmonise to facilitate true interagency collaboration— long before finding themselves forced to deal with such issues during a foreign deployment or national emergency. The work of the Center is primarily focused on training, education, and research related to interagency collaboration, complex national security challenges, and other public

policy problems for mid-career policy professionals and military officers. The Center also brings together leaders from all levels of government and the military for symposia, discussions, and projects to promote creative, collaborative solutions to emerging issues.

WILLIAM & MARY GLOBAL INNOVATION CHALLENGE

The William & Mary Global Innovation Challenge (WMGIC) encourages and facilitates interdisciplinary collaboration and applied learning opportunities among students, policymakers, practitioners, and researchers by bringing innovative and sustainable perspectives to solve complex global issues.

Established in 2017, WMGIC provides undergraduate students worldwide a platform for open collaboration and discussion with peers, faculty, and knowledgeable professionals to analyse and create sustainable and scalable solutions to challenges ranging from international and sustainable development to cybersecurity. The competition increases students' knowledge of and experience with the case study, design thinking, holistic sustainability, innovative processes, and policy entrepreneurship. Teams of three to five work with mentors and present proposals to industry judges. Top teams are chosen as finalists, give public presentations, and receive cash prizes.

WMGIC is a recognised student organisation at William & Mary and featured by the UN Sustainable Development Solutions Network, International Conference on Sustainable Development, and NATO Allied Command Transformation.

To learn more about this Challenge or engage with us, contact wmcoe@wm.edu.

Disclaimer

TABLE OF CONTENTS

LETTER FROM THE EDITORS

The NATO Alliance faces many threats, whether from the deployment of troops along strategic borders or the spreading of false information online to disrupt societies and undercut the central tenets of good governance. Enemies are visible across a battlefield, cloaked behind a computer screen, or even non-existent bots. Preventing incursions and mitigating damage not only requires the best minds operating inside governments and commands, but involves a whole of society approach to bring diverse perspectives and entrepreneurial approaches to the challenges of today.

NATO Allied Command Transformation (NATO ACT) Cyber Space Branch joined forces with William & Mary's Global Innovation Challenge (WMGIC) and Whole of Government Center of Excellence (WGC) to task a different cohort to tackle the problem of disinformation and election interference in member nations—in addition to the coders and colonels, undergraduate students from across the Alliance. In the first competition of this size and scope, 56 teams from 52 universities signed up to develop their recommended solution to how to best address election meddling. On November 12, 2021, the teams dissected the problem and crafted their approach over the course of six hours and in consultation with expert mentors from NATO member nations. Each was judged by a two-person panel on the following criteria: feasibility & effectiveness, creativity, privacy, sustainability, and fiscal pragmatism. The list of distinguished mentors and judges is contained here within.

Seven teams were selected as the winners of their streams owing to their unique and tangible recommendations. To thrive in the age of digital diplomacy, NATO Potato (University of Calgary, Sciences Po, and Leiden University) suggested that NATO ACT adopt an institution where NATO can identify and debunk the spread of disinformation. Belt & Road (Tufts University, University of Oxford, and the London School of Economics) recommended that NATO ACT develop the "Z Program" to reduce the demand for disinformation by limiting the impact of the wider public. CyberOps (Cambridge University, Staffordshire University, University of St Andrews, William & Mary) proposed a three-tiered system that can be used on their own or as a set of steps to follow, whereas each tier contains a two-pronged approach to combating disinformation through the use of public education and digital measures. LPR (George Mason University) developed a multi-faceted solution using machine learning, computer vision, and blockchain that ensures company security on a global spectrum while combating the problem at hand. The Net-Tech Warriors (Old Dominion University) suggested that NATO combat the destabilising effects of disinformation on NATO partner countries by aggregating in Norfolk media information from edge and vulnerable countries and analysing this information in real-time using existing technologies such as AI-FELIX and Synthesio. The Cyberian Huskies (University of Texas at San Antonio) recommended that NATO ACT create a Disinformation Collaboration Task Force of experts who would be responsible for aiding in the response of nation-states' disinformation threats. Lastly, the International Strategic Capacity Council (University of Calgary) recom-

mended the implementation of a specialised NATO council to be in reliable operation that deals with reports from member states about threats of disinformation during times of vulnerability and polarisation.

That said, all teams gave practical and sound advice to NATO ACT Cyber Space Branch. Therefore, the pitches of all the undergraduate teams are contained in this publication. Their ideas are all worthy of public distribution and may well aid in the development of government policies and practices. Should you find an item worthy of inclusion in your work, we ask that you do so with attribution. After all, this generation is our brightest yet.

We also thank our chief supporters, including the Cybersecurity Youth Apprenticeship Initiative (CYAI), the Studio for Teaching and Learning Innovation (STLI), and the Reves Center for International Studies.

Together, military leaders, policy practitioners, and students will proactively safeguard the freedom and security of NATO members for the next 70 years, regardless of the next hack or deep fake.

Kathryn H. Floyd
Kate Hoving
Tyler Lawrence
Thomas (Huan-Cheng) Liu
Nathaly Perez
Piret Pernik

PART I:
Participants and Partners

Participants and Partners

56 TEAMS FROM 52 UNIVERSITIES

PARTICIPATING UNIVERSITIES

Antalya Bilim University (Turkey)
Ashland University (United States)
Baylor University (United States)
Bryn Mawr College (United States)
California State University Maritime Academy (United States)
Cardiff University (United Kingdom)
Dokuz Eylül University (Turkey)
George Mason University (United States)
Hamilton College (United States)
Hofstra University (United States)
Hood College (United States)
Humboldt Universität Berlin (Germany)
Indiana University Bloomington (United States)
Johns Hopkins University (United States)
Keele University (United Kingdom)
Kenyon College (United States)
King's College London (United Kingdom)
Leiden University (Netherlands)
London School of Economics (United Kingdom)
Middle East Technical University (Turkey)
Muskingum University (United States)
Nottingham Trent University (United Kingdom)
Old Dominion University (United States)
Pepperdine University (United States)
Queen's University (Canada)
Sciences Po (France)
Simon Fraser University (Canada)
Stanford University (United States)
Stony Brook University (United States)
Swarthmore College (United States)
Technische Universität Berlin (Germany)
Tufts University (United States)
University of Calgary (Canada)
University of Cambridge (United Kingdom)
University of Edinburgh (United Kingdom)
University of North Carolina at Chapel Hill (United States)
University of Oxford (United Kingdom)
University of Southern California (United States)
University of St Andrews (United Kingdom)
University of Texas at San Antonio (United States)
University of Warsaw (Poland)
University of Western Ontario (Canada)
William & Mary (United States)

JUDGES AND MENTORS

Alex Anvari
Ecosystem Expert, Oracle

Peter Apps
Executive Director, PS21 and Global Affairs Columnist, Reuters

Mateusz Buczek
Capability Engineer, NATO ACT

LTC Devon Cockrell
Plans Officer, United States Army Pacific-Support Unit, Daniel K. Inouye Training Complex

Joey Cusimano
Cyber Software Engineer, Cybersecurity Youth Apprenticeship Initiative

Lisa Dickson
Senior Account Executive - Defence, Security, Public Safety and Intelligence Portfolio, Google Cloud

Dr. Alberto Domingo
Technical Director, Cyberspace, NATO ACT

Commander Davide Giovannelli
Researcher, Law Branch, NATO CCDCOE

Iria Giuffrida
Professor of the Practice of Law, W&M Law School

Prof. dr. Włodzimierz Gogołek
President of the Information Refining Center, Spin Off of Warsaw University

Dr. Kira (Hutchinson) Graves
GG-15 Intelligence Specialist (0132), G-2, U.S. Army Training and Doctrine Command

Lieutenant Colonel Matt Horton
G2 Opposing Forces Program Director, U.S. Army Training and Doctrine Command

Aron Hubbard
Director, Cybersecurity, Cybersecurity Youth Apprenticeship Initiative

Joshua C. Huminski
Director, Mike Rogers Center for Intelligence and Global Affairs at the Center for the Study of the Presidency & Congress; Visiting Fellow, George Mason University National Security Institute

Dr. Pedro Jerónimo
Head Researcher, MediaTrust.Lab, University of Beira Interior

Dr. Irini Katsirea
Reader in International Media Law, Director of Research, Centre for Freedom of the Media Communication, Media and Journalism Research Group, Journalism Studies, University of Sheffield

Antoine Landry
Cyberspace Federation and Partnership SME, NATO ACT

Dr. Birgy Lorenz
Scientist, Tallinn University of Technology

Dr. Elizabeth Losh
Professor of English and American Studies, W&M

Trish Martinelli
Regional Director, At Large, National Security Innovation Network

Keith Masback
Principal Consultant, Plum Run LLC

Robert McMath
Senior Consultant, JANUS Research Group

Ana C. Rold
CEO, Diplomatic Courier

John Scott
President, Ion Channel

Chris Shenefiel
Principal Engineer, Cisco Systems and Faculty, Computer Science, W&M

Dr. Anthony Stefanidis
Professor of Computer Science, W&M

Dr. Elis Vllasi
Lecturer, Simon Fraser University

Roger Yee
Managing Partner, Outcome/One

Lincoln Zaleski
Transparent Development Footprints, AidData

PARTNERS

Whole of Government Center of Excellence

Cybersecurity Youth Apprenticeship Initiative

The Studio for Teaching and Learning Innovation

The Reves Center for International Studies

PART II:
Agenda and Case Study

WMGIC x NATO ACT Cybersecurity Challenge Event Schedule

12th November 2021

Opening Ceremony 8:00 - 8:20 A.M. E.S.T.

Keynote Address by COL Bernd Hansen
NATO ACT Cyberspace Branch Head

The Honorable Kathleen T. Jabs
Acting Secretary of Veterans and Defense Affairs
Commonwealth of Virginia

Dr. Stephen E. Hanson
Vice Provost for Academic and International Affairs
William & Mary

Thomas Liu
President, Global Innovation Challenge (WMGIC)

Nathaly Perez
Global Innovation Challenge (WMGIC)

Nick Berklan
Global Innovation Challenge (WMGIC)

Mentoring Session Period 8:30 - 11:00 A.M. E.S.T.

The livestream will be paused during this time period and will resume for the closing ceremony. Participants, judges, and mentors should refer to the event packet for the appropriate links.

Teams Submit Presentations 11:05 A.M. E.S.T.

The livestream will be paused during this time period and will resume for the closing ceremony. Participants, judges, and mentors should refer to the event packet for the appropriate links.

Presentations 11:20 A.M. - 12:40 P.M. E.S.T.

The livestream will be paused during this time period and will resume for the closing ceremony. Participants, judges, and mentors should refer to the event packet for the appropriate links.

Judging 12:40 - 1:00 P.M. E.S.T.

The livestream will be paused and will resume for the Closing Ceremony.

Closing Ceremony . 1:00 - 1:45 P.M. E.S.T.

Dr. Alberto Domingo
Cyberspace Technical and Industrial Relations Director
NATO ACT

Dr. Teresa Longo
Director of the Reves Center for International Studies
William & Mary

Case Document for Undergraduate Teams, Mentors, and Judges

[Released to Teams 10th November 2021]

Nick Berklan '22
William & Mary

OVERVIEW

The WMGIC x NATO ACT Cybersecurity Challenge consists of seven streams of competition based on a case. The case outlines a single cybersecurity topic or challenge statement that you will seek to answer within the competition parameters, with the vantage point and resources of NATO.

Teams will meet with two different mentors, for 15 minutes each, following the opening ceremony. Mentors are academic, industry, and NATO professionals with a wealth of knowledge and experience. Draw on their expertise and ask them questions as you see fit. Reminder, your time with them is limited so take advantage of it.

Solutions will be presented by each team via a three-minute verbal presentation and evaluated by a panel of professional judges from within the field of cybersecurity. Presentations will be judged by criteria listed later in this booklet. The winner of each stream will be chosen from each of the seven streams to give a three-minute presentation at the closing ceremony and receive a cash prize. All competitors are encouraged to network with judges and mentors during the competition.

CHALLENGE STATEMENT

How can NATO enhance cyberspace situational awareness and readiness in order to combat disinformation online, in particular on social media, where the threat is constantly evolving?

RULES AND PARAMETERS

Teams must design a plan of action a) that NATO could use considering its capability and administrative constraints, and b) with the goal of project consultation and implementation within a calendar year (12 months), noting that projects should be at least feasible beyond the first year, and preferably scalable. Plans of action should be something that NATO can take forward.

The case introduced below will contain background information, but additional preparatory research is permitted and recommended.

Teams may not enlist the assistance of anyone on the WMGIC team, judging panel, faculty advisors, friends, or from any contact whose ideas are not publicly available (i.e., published online), other than their assigned team mentors.

Teams have from the beginning of mentoring sessions (8:30 am ET) to the deadline (11:05 am ET) to work on their project and create all deliverables.

DELIVERABLES

All teams will:

- Submit a five-slide maximum PowerPoint/PDF slide deck including a slide with a 150-word project summary by 11:05 am ET.
- Present a three-minute (maximum) PowerPoint presentation to the judges, including action item(s), outputs, potential NATO ACT implementation, and the 150-word project summary slide.
- Participate in a three-minute Q&A session with the judging panel.

The winner of each stream will present their three-minute pitch in front of high-level guests, other teams, and spectators during the Closing Ceremony. This should be the exact same presentation given previously to the judges.

JUDGING CRITERIA

Each criterion is equally weighted.

- Feasibility & Effectiveness: Is this a potentially effective solution to address the problem? Does the plan follow the rules and regulations of the competition (i.e., budget, scope)?

- Creativity: Do solutions show strategic thinking that utilises resources in inventive ways? To what extent is the solution differentiated from traditional approaches? Or how does it build off traditional approaches for that matter? What are the unique technologies that drive this approach?

- Privacy: How can you keep the privacy of online, in particular social media, users while still analysing public-contributed content? How will you

address the privacy and/or safety concerns of the public when it comes to the actions of nefarious actors online in these situations?

- Sustainability: Does this project have sufficient capabilities to continue into the future if it cannot fully meet its objectives on its base performance period? Does the project have performance metrics and evaluation incorporated into its plan? Does the solution have the potential for future growth?

- Fiscal Pragmatism: What is the cost-benefit analysis of the project? Does it make responsible use of funding? Will projections show its economic viability? Does the project have any return value? How do costs project out beyond the first year?

CASE INTRODUCTION

The following case is a prime example of disinformation being used in contemporary political affairs and is a situation we can learn from to further develop NATO's cyberspace situational awareness and readiness. Use it to assist in the formulation of your plan of action which responds to the Challenge Statement. Your plan of action does not need to restrict itself to Russia and Ukraine.

Case Background: The Roots of Political Tension Between Russia and Ukraine
The history of both nations dates to the Kievan Rus' civilisation, which existed from the 9th Century until the 13th Century, when the Mongols invaded. That both Russia and Ukraine claim the same ancestral homeland is the foundation of the connection between the two nations. Over time, a dynamic grew between the states in which Russia saw Ukraine as its smaller, inferior sibling. Russia, therefore assumed the right to exert political sovereignty over Ukraine when the two nations co-existed. Its policies of control over Ukraine continued into the modern era. When Joseph Stalin was the Premier of the USSR, he halted "indigenisation" policies that were meant to support non-Russians, initiating a new tone towards the group. Not long after, he began the infamous Ukrainian Famine (1932-1933) which killed approximately 3.5 million people. By the 1970's, the Ukrainian language could no longer be spoken or taught in schools in the Soviet Union. Ukrainian discontent with being controlled by a Moscow-centric government continued through the dissolution of the USSR.

When voting for the future of Ukraine after the fall of the USSR, the outcome was remarkable: more than 90% of Ukrainians voted for independence. This was highly worrisome to Russia. While parts of Ukraine were viewed by Russians as part of their homeland, Ukraine had also produced 25% of Soviet agricultural goods, economic output that would no longer be in Russian control. This vote also set the stage for the preeminent conflict in Ukraine in the post-Soviet Union era: the conflict between Western and Russian influence

in Ukraine. Because Ukraine is of great economic value to Russia, the Kremlin wishes to keep Ukraine in its sphere of influence and benefit from a close economic and political partnership. However, much to Russia's dismay, Ukraine looks westward to the rest of Europe and towards NATO.

Russia, pressured by the fact that Ukraine was slowly slipping out of its grasp, needed to find a way to stop this process. To achieve this, Russia looked to influence Ukrainian elections to make the outcome favorable to Russia and bring Ukraine more strongly under its grasp. In 2004, this tactic was first exposed during the Ukrainian presidential runoff election. The pro-Russian candidate, Viktor Yanukovych, was initially declared the winner in what was widely perceived to be a rigged election. Public outcry sparked protests across the nation which became known as the Orange Revolution. After a free and fair election a few months later, the pro-Western candidate, Viktor Yushchenko, won.

Russian Election Influence post-Orange Revolution: A Transition to Cyberspace

After the widespread reports of election tampering in 2004, the following election cycles in 2010 and 2014 were considered relatively well-run. In 2014, Ukraine adopted an information technology model for election monitoring, bringing their polling (vote-tallying) into a new frontier: cyberspace. The new development was exploited quickly when Russian cyber attacks compromised the Central Election Commission network. As mentioned earlier, these attacks occurred, but were caught or resolved before they could be detrimental to the election. Separate from the election, during the Crimean conflict in 2014, Russia conducted ongoing information warfare against Ukraine. It was one of the first real documented cases of the employment of cyber deception and influence in military operations. These operations were only a sign of what was to come during the ensuing round of presidential elections in 2019 as Russia's cyber tool kit continued to develop.

The election of 2019 was a race between the incumbent Petro Poroshenko and Volodymyr Zelensky, a former comedian/actor who owned a media production company. The two candidates were similar in their policy agendas, and both were favorable to Western ideals and alliances. However, a key distinction was that Zelensky felt that the decision should be left for the people to vote on, whereas Poroshenko wouldn't leave it up to the populace. After a campaign trail of roughly four months, Volodymyr Zelensky won both the general and runoff elections by 2.7 and 9 million votes respectively, making him the new President of Ukraine. Many felt that this election clearly showed the prevailing dissatisfaction with the incumbent Poroshenko.

Like the election before it, cyberspace was used to try to influence the outcome of the election in 2019. In this case, attacks weren't aimed at the election systems in Ukraine, but rather at the Ukrainian populace, reflecting a transition from cybersecurity attacks into disinformation warfare. Russia engaged in a steady flow of disinformation campaigns with the hopes of in-

fluencing the opinions of the Ukrainian public about their presidential candidates and dividing the nation. Disinformation, as defined by NATO is "the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead."

The Russian disinformation effort was ubiquitous. Unlike other disinformation campaigns that Russia has taken over the past half-decade, this one did not have a specific target or outcome in mind, nor did Russia favor a particular candidate or party. Russia delivered a narrative in the disinformation that the election results needed to be questioned because they were illegitimate or rigged. In essence, the propaganda was being used to discredit the legitimacy of Ukraine's democratic processes, as well as discrediting the State itself. Considering the new importance of social media discovered by Ukrainian Presidential candidates, covered later in this document, and the myriad of online activity in the run up to, during and after the election, the situation was ripe and aspects of Russian disinformation campaign tactics are all over.

Russian Tactics

Disinformation has been a key part of the Russian covert operation toolkit. The word disinformation (дезинформация – dezinformatsiya) itself originates from Russia in the 1920s when the police began the practice of disseminating false information with the intent to deceive public opinion. Interestingly, the term didn't reach English dictionaries until the 1980s. Russia has developed a clear methodology for disinformation campaigns. They start by pinpointing socially and/or politically polarising issues. Then, false narratives are built to drive a bigger wedge between already polarised sides and are made and disseminated through established networks of influence. From that point forward, the main goal of the campaign is to create confusion amongst the targeted group, while trying to conceal the origins of the disinformation. The final part of the campaign is to amplify the messaging by saturating information spaces -- like social media -- with posts to further sow doubt and uncertainty. In recent years, because of social media, disinformation campaigns have hopped online due to their increased ease and effectiveness.

During the 2019 Ukrainian election, a new Russian disinformation tactic emerged on Facebook. The Kremlin was finding Ukrainian citizens who would sell them their Facebook accounts, which would be used to promote political ads or post fake news. The emergence of this new tactic did not mean that old tactics were disregarded, however. Russia amplified and adapted their disinformation tactics to cyberspace. By paying real Ukrainians to do their bidding, Russia more effectively conceals the origins of the disinformation. In the January preceding the election, Facebook removed approximately 150 fake accounts from the site that reportedly mimicked a disinformation campaign carried out against the United States the previous year. Two months later in March, the social media platform removed an additional 2,000 accounts, pages and groups tied to Russia, some of which had targeted Ukraine. These instances of going through and removing malicious accounts/groups/

pages is an attempt by Facebook to reduce some of the amplification of Russian disinformation on its platform.

Russian tactics are also taking advantage of the embedded algorithms in social media platforms to help disseminate disinformation. These algorithms determine what posts a user sees and interacts with and recommend content similar to that in the future. This creates an echo-chamber effect where pro-Russian leaning Ukrainians will almost assuredly be inundated with pro-Russian propaganda, and vice versa for pro-European Ukrainians. This actively aids in the political polarisation process, which only works to Russia's disinformation plan by creating a divided Ukraine. In other words, the algorithms already embedded in these social media platforms do the work of "amplification" for adversaries, in this case Russia, without involving any effort on their behalf.

Politics and Social Media in Ukraine

Social media have become increasingly important in Ukraine's political races, arguably integral to the process of running a political campaign. As mentioned before, President Zelensky was an actor before his political career. In fact, he played the Ukrainian President in a TV show, Servant of the People, which also became the name of his political party. Equipped with this background, Zelensky and his campaign team used social media to their advantage and deviated from the precedent of bland and factual internet presences. Instead, Zelensky made a conscious effort to humanise himself and evoke emotion by showing aspects of his personal life, or even simply taking selfies. The political party Holos, a small minority party within Ukraine, further illustrates the importance of social media in Ukrainian elections. After a late entry into the race, the party invested their resources in social media and won parliament seats in an election upset.

Apart from more official political action taking place on social media, Ukrainian users themselves are making social media more politicised. From May 1 to September 15, 2019, Facebook saw an 8.2% increase in Ukrainian users who posted about political parties and parliament. This shows that politics are becoming more of a salient issue on social media. A metric to gauge the polarisation of Ukrainian social media, in particular on Facebook, is the reaction function. The reaction function allows a user to express positive, negative or neutral sentiments about a given post. Based on a survey that was conducted over two sample periods, no party received over 25% positive reactions. It is generally the case that parties received a higher percentage of negative reactions than positive ones, conveying the prevailing theme of polarisation.

Grievances

Even though Facebook was taking an active role in monitoring for false accounts and groups, there are claims it did not take enough strides to make real accounts discernable from the droves of false accounts trying to undermine their work. For instance, the personal account for candidate Zelensky

was verified by Facebook, but his campaign's account was not. The head of digital strategy for the candidate, Mikhail Federov, says that because of this, the campaign's page is drowned out by fakes that are nearly identical to the real one. In response to Facebook's short-coming, Zelensky's campaign had to create a group that alerts the candidate's followers to fake accounts.

Furthermore, Facebook was admonished for a lack of situational awareness. Less than two weeks before the election, the company introduced a new tool meant to increase transparency around political advertising. With full knowledge of when the Ukrainian election was going to occur and what was likely going to happen on their site in the run up, Facebook was being criticised for the poor timing of the roll out of these tools. These shortcomings highlight the importance of coordinating with private companies to ensure effective and cohesive cyber policy and defence. Additionally, the existence of algorithms and reaction functions creates two points of worry. These capabilities allow Facebook to analyse content, which create privacy and censorship issues.

While elections take place at distinct moments in time, Russian disinformation campaigns are continuous, shaping the opinion landscape to serve whatever intermediate goals the Kremlin has identified, as it works towards its longer-term goal of regaining control of Ukraine. This information warfare crosses geographical boundaries, has no start or end date, and is often manifested in the form of multiple concurrent disinformation campaigns, seemingly unrelated, but sharing the common goal of eroding confidence in institutions of democracy around the world. In conclusion, information warfare, leveraging cyberspace as a key vehicle, can also be coupled with more traditional warfare tactics (i.e. kinetic) to achieve military objectives as part of hybrid campaigns.

William & Mary Cybersecurity Challenge with NATO ACT Draws Students from 43 Universities Worldwide

Kate Hoving
W&M News, 1st December 2021

On Friday, November 12, for six exciting hours, the Reves Room was transformed into Command Central for William & Mary's Global Innovation Challenge (WMGIC) x North Atlantic Treaty Organization (NATO) Allied Command Transformation (ACT) Cybersecurity Challenge. Underneath the portraits of Emery and Wendy Reves and Frank Shatz, just a few feet from the signed letter from Albert Einstein, just under two dozen student volunteers sat with their laptops at tables. Their headphones and mics on, they monitor their respective teams, quietly issuing instructions, timing presentations and shepherding mentors and judges in and out of their breakrooms. They represented different majors and varying levels of experience with WMGIC, but they worked like seasoned pros, unflappable, able to speak in hushed but assertive tones and totally dedicated to following their assigned team from beginning to end of the competition.

Thomas Liu directs the volunteers in the control room (Credit: Tyler Lawrence).

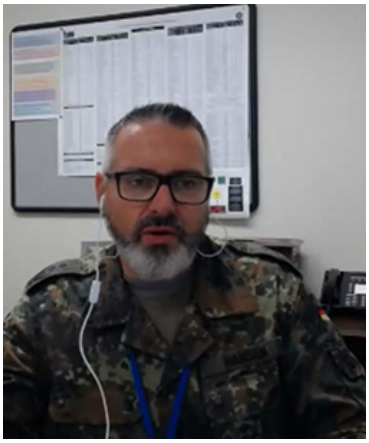
The podium and banner were in place, as was the video camera for recording the introduction and closing ceremonies. WMGIC directors moved quietly from station to station, checking progress and offering guidance when necessary. Tyler Lawrence from the Reves Center was stationed at the back of the room, managing the webinar and photo documentation. Dr. Kathryn Floyd 05, Director of the Whole of Government Center of Excellence, served as host and staff, monitoring the presentations and pitched in as a mentor when necessary, seamlessly switching gears but never losing her characteristic high energy and enthusiasm.

When the event went live at precisely 8am ET, Thomas Liu 22, President of WMGIC and emcee of the opening ceremony announced to a worldwide audience via Zoom, "Together, our participants, judges and mentors represent over 16 countries across the NATO alliance spanning over 11 time zones from California, where it is currently 5am and Turkey where it is already 4pm."

Liu was followed by Vice Provost of Academic and International Affairs Steve Hanson, who helped to give some William & Mary context: "This is a perfect event for William and Mary. We are in many ways Americas first global university, having been founded in 1693 by King William and Queen Mary. We are also a military friendly university and we enjoy wonderful partnerships with our military and federal colleagues across the country. And now across the world too. This event also represents William and Marys interest in student empowerment. We are a student driven university in many ways and this event is largely organized by our students. We now know that you around the world are participating in that same kind of student innovation experience, which we are really proud of."

Hanson then introduced Kathleen T. Jabs, Virginias Acting Secretary of Veterans and Defence Affairs, who reinforced the importance of the topic of the competition: "Our Virginia National Guard cyber teams are on alert to help cities and localities around the Commonwealth. I am very grateful that such young minds and bright minds are gathered together to work on this problem, and I commend you all for your dedication and to seeing what type of solution you come up with to battle misinformation. It is definitely a problem for our times."

Above: Thomas Liu; Stephen E. Hanson; Kathleen T. Jabs. Opposite: Col. Bernd Hansen.



Col. Bernd Hansen, NATO ACT Cyberspace Branch Head, delivered the keynote and gave the students, mentors and judges their marching orders: "Today we are looking forward to hearing the voices of our youth, to benefit from fresh thoughts and new ideas. Todays challenge aims at interdisciplinary collaboration to create innovative solutions for current global issues. NATO and its allies need to constantly adapt, transform, and increase resilience in cyberspace. Please do not hesitate to be bold and disruptive in your proposals and recommendations while bearing in mind the actionability and feasibility."

At 8:30am ET, the ceremonial obligations fulfilled, now came the truly challenging part: The competition had begun.

A firm foundation but a new direction

On October 14, when WMGIC announced its partnership with the Whole of Government Center of Excellence and NATO Allied Command Transformation (ACT) to hold the first WMGIC x NATO ACT Cybersecurity Challenge on disinformation and election interference in the cyber realm, there were hopes that they would elicit a good response from student teams. But it was a new venture for all partners involved, and they tried to keep expectations realistic. After all, the partners brought proven— albeit different—strengths to the venture.

Established by students at William & Mary in 2017, WMGIC has successfully presented intercollegiate case competitions encouraging interdisciplinary collaboration for five years, but the cyber security element was new.

"WMGIC has historically focused our annual case competition around international and sustainable development, so the new partnership with NATO ACT through the support of the Whole of Government Center of Excellence is indeed unique," says Liu . "We were thrilled that NATO ACT was interested in partnering with WMGIC on the event and its willingness to review students innovative proposals after the event to determine its relevance for NATO and the policy community writ large."Kay Floyd working with a mentor
Kay Floyd working with a mentor

The reason for the inclusion of NATO ACT and the broadened focus for WMGIC came from Kay Floyd. "I have admired the WMGIC leadership ever since we interacted during a Whole of Government course. Their core challenge model addresses sustainable development problems, which is an essential component of international security," says Floyd. "With NATO ACT, we were looking for a way to have senior level policy makers interact with

fresh—indeed undergraduate—ideas related to combating disinformation. It was a natural fit to pair WMGICs model with this a different global problem, cybersecurity."

For NATO ACT, the collaboration also made sense. At the announcement of the challenge, Dr. Alberto Domingo, ACT Cyberspace Technical Director, explained their reasons for establishing the partnership: "ACT is NATOs warfare and capability development Command, leading the military adaptation and transformation of the Alliance to ensure it is capable of meeting the challenges of today and tomorrow. We work very closely with a wide range of stakeholders (from NATO bodies, Nations, Industry, Academia, etc.) to guarantee that NATO remains fit for purposes in the cyber realm. Partnering with William & Mary—especially on this event with WMGIC and the Whole of Government Center of Excellence—promises to enhance our network and creative capabilities."

The three partners were on board, but whether this new competition would attract a significant number of students, universities and mentors was not clear.

The call went out for participants: It was open to undergraduate students in universities nationwide and internationally from NATO Member Nations. Each team was comprised of three to five students. All levels of experience, and all majors were welcome. One caveat: The entire event would be conducted in English.

A multiplier effect
Any concerns about low interest were quickly allayed.

As a benchmark, previous WMGIC hackathons have hosted on average 20 to 30 teams of undergraduates, a respectable number, although they hoped for maybe 40 teams.

Working through the usual WMGIC contacts, but now amplified by Whole of Government and NATO worldwide contacts as well as the Global Education Offices exchange partners resulted in an unforeseen multiplier effect.

Nearly 300 undergraduates from 53 universities worldwide applied to compete, with several teams formed in the last 24 hours before the start of the competition.

"We were overwhelmed by the interest and positive response from students not only in Virginia and the United States but across the entire NATO Alliance," said Nathaly Perez 22, co-director of the Challenge. "As a result, our team had to expand the events capacity by adding two streams (16 teams) within the last week to a total of 56 teams competing."

The 56 teams were organized in seven streams (named, appropriately per NATOs phonetic alphabet, Alpha to Golf). There was ultimately a waiting list.

Increased diversity and access
In addition to the expanded network for outreach, the virtual nature of the competition also enhanced participation and diversity. Teams were formed both within and across both universities and national boundaries.

And the universities represented truly were global, ranging from: Ashland University to Antalya Bilim University (Turkey); California Maritime to Cardiff University (United Kingdom); Hamilton College to Humboldt Universität Berlin (Germany); Stanford University to Sciences Po (France); University of Texas at Dallas to University of Warsaw (Poland), and so many more.

The cross-university teams were organized by the students themselves, based on previous connections. A few applicants did not have teams, so WMGIC created a team for them, made up of students from William & Mary, Cambridge University, and the University of St Andrews. The participants named their team "CyberOps."

For Camilla Yeleussizova '22, a public policy major, it was her first time participating in a WMGIC event: "I wanted to dip my toe into cybersecurity, as I am considering my future prospects. I requested to be added to a team since I applied by myself, so this was my first time meeting my teammates." It was a new experience for her on all fronts, but she was glad she participated. "I did not know what to expect of the day but I was pleasantly surprised."

Her teammate Justin Cresent '25, was enthusiastic from the start. "I have a passion for cybersecurity and plan to pursue it as a career. This event came into my inbox and I jumped at the opportunity to take it. I loved the experience and hope to bring even more to the table in years to come!"

Camilla was not put off by the cross-university team. "It was gratifying to work with a diverse team, I appreciated the inclusivity of the event, those that had no teams were able to participate as well. The virtual format was cool, as it allowed ease of communication and participation for those all over the world."

Justin embraced the whole experience and is ready for more: "I love my teammates, the challenge statement, and all the mentoring and questions asked by the judges. Participating in WMGIC was an experience I really enjoyed. I did not know what to expect going into it, but as I collaborated and worked through challenges with my teammates I had so much fun and learned new perspectives about our world and others takes on how to handle cybersecurity issues. Overall, this experience was amazing, and I will for sure be participating again!"

Judges and mentors bring expertise and guidance
The expanded network from the collaboration resulted in a wide-ranging group of judges and mentors who volunteered their time and expertise to the competition.

Judges Prof. Iria Giuffrida (W&M Law) and Dr. Alberto Domingo (NATO) confer.

"The event went way beyond our expectations in every possible way, not just in the participation from students across the NATO alliance, but also in the highly qualified slate of judges and mentors from the media, academic, private industry, and military communities," exclaimed Perez.

Some of the organizations represented include NATO ACT, NATO CCDCOE, Estonias Tallinn University of Technology, Cisco, Google, U.S. Army training and Doctrine Command, and among many others.

Floyd explains the value of these kinds of mentors in the competition is not just for students but for the experts, too. "The payoffs are immeasurable. Mentors have the opportunity to apply their expertise in unexpected ways and to have their views impacted by the world as seen by a 20-year-old university student. This cycle of interaction elevates and refines all ideas, building intergenerational networks of thinkers and practitioners. And it is really fun to participate in these challenges."

Lisa Dickson, Senior Account Executive - Defence, Security, Public Safety and Intelligence Portfolio, Google Cloud, voiced a common motivation of the judges and mentors: "I encourage young adults to take action and get involved in issues that matter to them. Seeing the students initiative and interest is refreshing."

When a mentor was a little late in logging in, Floyd was also able to step in briefly. "I loved it!," she recalls. "Being a mentor allowed me to encourage the students to think in terms of feasibility and practicality, in addition to coming up with a brilliant idea."

The competitions challenge and run of show
The participants were issued the following Challenge Statement:

> *How can NATO enhance cyberspace situational awareness and readiness in order to combat disinformation online, in particular on social media, where the threat is constantly evolving?*

Nick Berklan '22 drafted both the challenge statement and the case study supporting it. It was a model for any case study or executive summary — detailed, extensively researched, with references and suggestions for more details:

"The case I composed is about Russian information warfare during the Ukrainian election of 2019. It is an exemplary case of how social media is playing an increased role in information warfare. However, the case was merely a primer to engage the minds of the teams about the issues at large posed in the challenge statement. It was my hope that teams would take these things and formulate innovative solutions that NATO could potentially use moving forward."

Teams had to design a plan of action a) that NATO could use considering its capability and administrative constraints, and b) with the goal of project consultation and implementation within a calendar year (12 months), noting that projects should be at least feasible beyond the first year, and preferably scalable.

The criteria for judging were equally weighted among the following: Feasibility & Effectiveness; Creativity; Privacy; Sustainability; and, Fiscal Pragmatism.

Their final deliverable would be a presentation to judges with five slides maximum and a 150-word project summary.

Starting promptly at 8:30am ET, each team began consulting with the two mentors assigned to their stream in 15-minute sessions. The mentors met separately and thanks to differences in styles, temperament and backgrounds, gave a variety of suggestions and guidance. They did not hesitate to question and call out inconsistencies and oversights. Some of the common issues that arose included potential overreach –did their idea really fit within NATOs mission--as well as potential costs. Transparency of information as well as the potential use of AI and blockchain were introduced. Building trust was also a common theme, as well as discerning the audience and constituents for the proposals.

At 11:05am, teams presented their 150-word summary and then judging began at 11:20am. The seven streams were judged concurrently. Each team had three minutes to present, after which the judges had three minutes for Q&A and then four minutes for a private discussion to score the presentation.

At the end of the presentations, judges consulted their scores and made the final judgement of the winning team. The seven winners were reported to WMGIC and announced at the live closing ceremony at 1pm. Each team presented its winning proposal to the audience. The winners were awarded $500 virtually by Kay Floyd; Professor Teresa Longo, Executive Director of the Reves Center; Liu and Perez Rojas.

The Winners:

- Alpha Stream: Team NATO Potato (University of Calgary; Sciences Po Paris; Leiden University)
- Bravo Stream: Team Belt & Road (Tufts University; University of Oxford; London School of Economics)

- Charlie Stream: Team CyberOps (Cambridge University; University of St. Andrews; William & Mary) (Note: This was the team that WMGIC created from individual applications)
- Delta Stream: Team LPR (George Mason University)
- Echo Stream: Team Net-Tech Warriors (Old Dominion University)
- Foxtrot Stream: Team Cyberian Huskies (University of Texas at San Antonio)
- Golf Stream: Team International Strategic Capacity Council (University of Calgary)

Hotwash and next steps
For the WMGIC team, this was both a learning experience and a success. "First of all, we learned not to underestimate ourselves. This event was not only double the size of any event that we have run in the past, but it also demonstrates WMGICs impact runs far beyond the walls of William & Mary, signifying our global reach," says Liu. "Second, the partnership with NATO ACT helps us realize our mission to connect students innovative solutions with the real world, moving forward, we hope to leverage the WMGIC network to secure such partnerships for our flagship spring event."

Floyd also was impressed with both the ideas generated and WMGICs execution of the event. "The WMGIC students were every bit as professional as the tabletop planners or wargamers in Washington, DC. With very little resources, they pulled together a massive international challenge with students as far away as Turkey. I would work with, and indeed for, them any day."

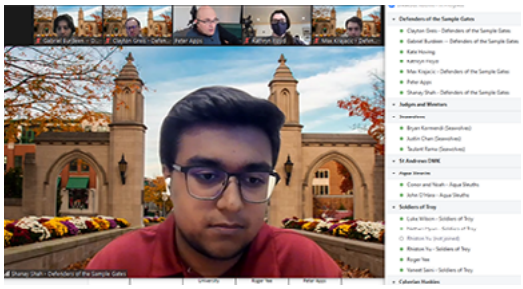
Dr. Alberto Domingo, Technical Director, Cyberspace, NATO ACT, and one of the Foxtrot judges, was also encouraged by the results and potential. In his closing statement, he remarked:

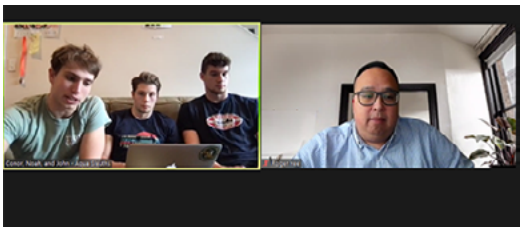
"The case study that you have been grappling with today is of at most importance for ACT and NATO. We consciously did not ask you to reflect on a science fiction of scenario, but rather on topics that are of strategic importance for NATO and its allies, and on which we need to act.

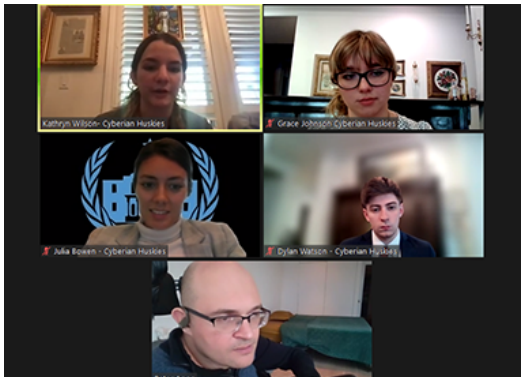
"NATO cannot do so in isolation. We need to foster partnerships, notably with academia, which is critical and this event today highlights I hope the multiple benefits of this kind of engagement."

"As one of the judges for this competition, let me tell you that I have been impressed by the quality of the action plans and recommendations that you have come up with. A number of ideas that were presented today were very innovative. Some of these ideas are definitely actionable and worth pursuing...So do not be surprised if you hear from us in the near future."

Photos opposite page, clockwise from top left: Defenders of the Sample Gates (Indiana University) during mentoring; Mentor Roger Yee mentors W&M Team Aqua Sleuths; In the control room; The winners were awarded $500 virtually by Professor Teresa Longo, Executive Director of the Reves Center; Kay Floyd; Perez Rojas and Liu; Kay Floyd working with a mentor; Managing the challenge; In the control room; Peter Apps mentors the Cyberian Huskies from University of Texas at San Antonio.






Kathryn Wilson- Cyberian Huskies
Grace Johnson Cyberian Huskies
Julia Boxen - Cyberian Huskies
Dylan Watson - Cyberian Huskies


1001
Date 11/12/2021
WMGIC
$ 500.00
Pay to the Order of Winners
00/100 Dollars
Jane Blumfeld
For WMGIC/NATO ACT
WMGIC
Authorized Signature

PART III:
Winning
Pitches

Winning Pitches

Stream: Alpha

TEAM NAME: NATO Potato

AUTHOR NAMES: Wei Azim Hung, Erica Peng, Cheng-Hao Howard Shen

AFFILIATIONS: University of Calgary; Sciences Po Paris; Leiden University

SUMMARY: To thrive in the age of digital democracy, NATO ACT should adopt an institution where NATO can identify and debunk the spread of disinformation.

PITCH: The question today is, in what ways can we provide an amicable solution which would produce tangible results in less than a year, that is cost-effective, replicable, scales well, and safeguards the privacy of citizens when campaigning against disinformation?

Thus far, NATO has been incompetent in terms of its participation in the world of digital democracy. To thrive in the age of digital democracy, you have to be willing to effectively engage in different ways, such as through images, videos, or pieces of text that could be quickly shared. More importantly, the message disseminated has to be recognisable, trustworthy, and humorous. We suggest that there is a positive pattern of exposure to political memes. Political memes have effects for rapid dissemination, increase civic engagement, and are effective in countering disinformation.

Our model aims to facilitate an environment that would engender digital democracy. It is a policy that produces immediate effects but also builds a robust environment combatting disinformation in the long run. To achieve this goal, we emphasise the element of co-creation as opposed to just media literacy.

Hence we introduce the institution of Media Environment Mediation and Empowerment System (MEMES).

- First, NATO will identify the disinformation being spread. It will then release a press statement providing accurate information to the press.
- Secondly, NATO would have a specialised department that creates debunking memes on its social media pages. In this regard, the meme is replicable, short, easy to understand, shareable, and has an element of humour within it.
- Moreover, NATO must have the capacity to respond to unsubstantiated claims in two hours.

The element of humour is indispensable for two reasons:

- First, we are effectively strategising humour in dismantling so-called "outlets of anger", which disinformation strives to manifest.
- Second, the internet is predominantly occupied with younger generations. Hence, by drawing that humorous connection, they are more likely to share these posts with not only friends but also family members that could be less media-literate. According to the trusted messenger theory, people are more likely to trust people they know and accept clarification from people they trust.
- Third, NATO would request its online followers and supporters to repost the meme. People are more likely to believe a piece of information if five criteria are met: compatibility with other known information; credibility of the source; whether others believe it; whether the information is internally consistent; and whether there is supporting evidence.

By taking the steps suggested above, NATO can propagate accurate information faster and provide clarification to the masses, faster than trolls who disguise themselves as the arbiter.

Stream: Bravo

TEAM NAME: Belt & Road

AUTHOR NAMES: Max Fu, Gary Guo, Lehan Guo, Ruowei Ji

AFFILIATIONS: Tufts University; University of Oxford; London School of Economics

SUMMARY: The aim of Z program is to reduce the demand for disinformation by limiting the impact on the wider public.

PITCH: **Overview of Z Program**

As the Russia-Ukraine case and multiple real-world examples suggest, disinformation gauges polarisation in public opinions and is damaging to society. Theoretically, there are two approaches to combat disinformation: to reduce the supply of disinformation by preventing it from occurring, and to reduce the demand for disinformation by limiting the impact on the wider public. Most political-military tactics that NATO currently adopts have focused on the former approach. Z Program, by contrast, adopts the latter to tackle disinformation. Z Program aims to improve situational awareness and readiness against disinformation by providing information on disinformation to the public. Z Program will collaborate with not only independent NGOs, academics, and think tanks, but also influential content creators such as stand-up comedians, artists, singers, writers. Z Program has three parts. The first part contains mainly fact-checking. The second part aims to provide monthly reports on current disinformation and common strategies against potential disinformation. The final part, which is the crucial part, is to provide interesting and easy content about disinformation, including videos, songs, and stories. Imagining a stand-up comedian joking about disinformation, that is how Z program wants to improve people's situational awareness and readiness against disinformation.

Course of Action

Z program consists of four stages. At each stage, we specify the implications which can be hopefully brought about, on both the institutional and the socio-psychological level.

Stage I. Studying Past Incidents (3 months)

- Action 1. Cataloguing past data, analysing trends
- Action 2. Forming case studies for educational purposes

Stage II. Overcoming Current Challenges (6 months)

- Action 1. Engaging the academia and media outlets to establish a platform for effort coordination

- Action 2. Instituting regular checking mechanisms and publishing reports on a monthly basis

Stage III. Future Prospects (15 months)
- Action 1. Professionalising the institutions by codifying information selection standards, standardising the selection process, and promoting information of higher quantity and quality
- Action 2. Expanding public influence gradually through the trickle-down effects in civil society

Stage IV. Consolidation and Positive Feedback (all-time) 3
- Result 1. Enhanced reputation and appeal through published attractive and high-quality information. More viewers, writers, and social media attracted. The platform's content quality and quantity further consolidated.
- Result 2. Expanded public influence among particular social strata. The free flow of information in democracies spreads the contents to the wider public. With the assistance of social media, the platform gained higher popularity. A remarkable improvement in the general level of public awareness.

Sustainability Check
NATO could further guarantee the sustainable functioning of Z Program by devoting resources to three actions. First, regularly revise the effectiveness of different tactics across the project. Second, based on the revision, apply and upgrade current metrics to accommodate an increasingly complex climate. Third, invest in data storage and handling procedures on data collected to protect privacy and delete past data on a regular basis, which would not necessarily affect the effectiveness of the project.

Concluding Remark
Z Program provides an ideal platform in which NATO's information datasets may be organised in a more systematic manner and stored for later references. They can also be utilised as educational resources to foster better social awareness. By coordinating efforts from a diverse range of players and stakeholders including the academia and media outlets, NATO achieves its main aim of engaging as many sections of the society as possible to attain a self-reinforcing positive feedback loop, in which the platform acts as an information provider and effort coordinator, and the civic society as both the content recipients and contributors. Polarisation caused by disinformation can be thus effectively minimised.

Stream: Charlie

TEAM NAME: CyberOps

AUTHOR NAMES: Jessica Poon, Milena Stefanovic, Camilla Yeleussizova, Justin Cresent, Emily Dubrovska

AFFILIATIONS: Cambridge University; Staffordshire University; University of St Andrews; William & Mary

SUMMARY: A three-tier set of recommendations, varying in degrees of cost, that addresses the educational and advertising aspects of spreading disinformation.

PITCH: Today the contours of the information landscape are evolving faster than ever. Technological advancement and social media have taken our society by storm, but we have been slow to adapt our laws and policies to mitigate the downsides of the sheer speed at which information can be disseminated. News and knowledge are everywhere in our age of connectivity, but "truth" and ways to verify it are in short supply. This whole-of-society issue is one which requires an equally holistic set of solutions.

In a sensitive ecosystem which can be engineered for nefarious purposes, we look to operationalise actors across the spectrum and mobilise both digital and civil tools in a new direction. Our proposal goes with the grain, towards principles of behavioural economics to build in greater critical thinking via intrinsically motivated behaviours. A global issue requires a global solution, rather than a solely US interventionist slant in regards to implementation and execution.

As with any ambitious project that wishes to incite societal change, we understand that financial limitations may be a major hurdle. This is why our recommendations are divided into cost-based tiers, to allow for responsible use of funding and provide NATO with actionable options, even if they do not wish to fully commit to some of our suggestions. These tiers can be used on their own or as a set of steps to follow, and each tier contains a two-pronged approach to combating disinformation through the use of public education and digital measures.

Tier I Recommendations
This tier is intended to be low cost and targets primarily English speakers due to the language's status as a lingua franca.

In order to make the general public more aware of how to combat disinformation, the education curriculum may be externally influenced by creating a webinar series for schools or universities on the topic of disinformation.

Additionally, local community influencers may be recruited to spread awareness of good practice. Both of these suggestions should be supported by social media advertisements to promote further awareness and education.

To protect the integrity of social media accounts, political accounts could receive an allocated team from NATO, and social media entities should be encouraged to utilise two-step verification and more scrupulous vetting during election periods.

Tier II Recommendations
This tier is intended to be medium cost. Speakers of languages in previous tiers are targeted, along with speakers of other common languages, such as Russian or Spanish.

To focus on the education of impressionable young people, the curriculum may be further influenced by scheduling touring talks at schools or universities on the topic of disinformation. Elevated levels of advertising can be used to further promote awareness and education.

Existing resources and infrastructure may be used to create positive feedback loops of information from verified sources, and partnering with fact-checking websites would create a holistic network under a NATO-set standard.

Tier III Recommendations
This tier is intended to be high cost and will have the highest impact. Speakers of languages in previous tiers are targeted, along with speakers of APAC region languages.

Sponsorships and massive marketing campaigns across billboards, buses, and cinema can be used to truly place disinformation awareness in the eye of the public. This will increase friction between the creators of disinformation and the users it reaches, as well as enable the public to reduce the influence of fake news outlets and other forms of disinformation.

Widespread, transparent, and standardised social media flagging algorithms can be used to assign information indices, such as a reliability score. The use of these algorithms by industry leaders may be incentivised with tax breaks or reputational responsibility.

Stream: Delta

TEAM NAME: LPR

AUTHOR NAMES: Likhitha Addagatla, Radha Kasarla, Meshwa Desai, Stuti Chaurasia, Saipriya Rachakonda

AFFILIATIONS: George Mason University

SUMMARY: A multi-faceted solution has been created using machine learning, computer vision, and blockchain that ensures company security on a global spectrum while combating the problem at hand.

PITCH: A multi-faceted solution has been created using machine learning, computer vision, and blockchain that ensures company security on a global spectrum while combating the problem at hand. The three-part solution is capable of addressing the issue of disinformation from a holistic viewpoint as follows:

1. Artificial Intelligence: Machine Learning

- Text mining will be used to collect data and text analytics to apply sentimental analysis as well as other algorithms to infer whether the information should be flagged as inaccurate or opinion-based. The algorithm would run through a post and if fact-based, an accuracy scale would be used to check for the reliability of the information. The information pulled from these algorithms will allow users to make informed decisions.

2. Artificial Intelligence: Computer Vision

- A computer vision algorithm will be created to detect pictures or videos that are being used as deep fakes. Images with text are also an extremely huge part of social media platforms, so Optical Character Recognition (OCR) can be used to analyse the text found in images to determine if the visual has been textually altered.

3. Blockchain

- Blockchain is immutable, allowing verification and re-verification, so it will ensure that content has not been modified, thereby helping re-establish trust in social media platforms. Blockchain will also keep track of the chain of custody by tracing back to the source of misinformation.

Implementation:

According to the NATO ACT implementation, the algorithm would be branched from the organisation, ensuring that social media companies are not to blame. This makes it important to pitch these ideas to different social media sites. Once the multi-part solution is implemented, the agile system development life cycle model will be used to directly deploy the solution to

the social media companies. Every period, the company will give feedback to make modifications and repeat the process. For the initial stages, the plan is to work with smaller platforms in order to redevelop the model that meets concurring requirements. Depending on the resources and funding, the partnership would be able to work with multiple platforms instead of one.

The proposed solution can ideally be implemented in a 12-month period using the agile model and sub-teams to work on each facet of the project. The different teams will be Machine Learning, Computer Vision, and Blockchain. These teams will be working simultaneously to help deliver the products in a timely manner. After 12 months, the design can be expanded to larger social media companies such as Facebook and Instagram. In order to get these companies on board, a trial period will be offered to provide data on how the technology is performing. The benefits of the solution include raising awareness and improving mental health by establishing trust across all social media platforms. The solution needs to be implemented at the earliest to minimise the cost of inaction.

In order to combat disinformation, the solution implements fact and opinion-based machine learning algorithms, computer vision using Optical Character Recognition, as well as blockchain for re-verification of the data. Keeping an agile model, a twelve-month frame will ensure scalability. Working with NATO ACT allows for collaboration with the government sector. This design will help raise awareness, re-establish trust in social media platforms, and push society to reflect on their opinions.

Stream: Echo

TEAM NAME: Net-Tech Warriors

AUTHOR NAMES: Olivia Hoernlein, James Sweetman, Gregory Wilson

AFFILIATIONS: Old Dominion University

SUMMARY: To combat the destabilising effects of disinformation on NATO partner countries, media information from edge and vulnerable countries can be aggregated by ACT in Norfolk and analysed in real-time using existing technologies such as AI-FELIX and Synthesio.

PITCH: The spread of disinformation on social media platforms has been, and continues to have a destabilising effect on NATO partner countries' populations and their election integrity. In order to best combat this problem, media information from edge and vulnerable countries can be aggregated by ACT in Norfolk and analysed in real time using existing technologies such as AI-FELIX and Synthesio. AI-Felix is already used in the NATO infrastructure, has quick processing times, is modular, adaptable, efficient, provides automated metadata extraction, and can deliver analytics on the data. Synthesio is a dashboard that can assist with providing clear and real time visual information about the data. Synthesio can be used to track and predict trends and attitudes in vulnerable populations as well as locate the sources of the trends. In terms of adopting these applications into the NATO infrastructure, the capabilities of these technologies can be rapidly upgraded with the TEXAS project framework so that they may quickly fill our needs.[1] Trends of disinformation can then be distributed to affected countries from centralised NATO command, and through partnership with cooperative social media platforms. Each country using this NATO SAR can then take actions that best suit their geopolitical climate, based upon SOPs that would be developed based on past effective actions. Costs of using existing technologies is minimal, and would include upgrades to existing data storage facilities in Norfolk.

We also encourage the using the blockchain as an active method to target disinformation. We can use this technology to verify digital media by authenticating publications, images, copyright, metadata, and general content to a digital registry.[2] This can prevent fake news distributors from co-opting

1 "NATO." ACT's Agile Process Delivers TEXAS Ahead of Schedule: NATO's ACT, September 18, 2020. https://www.act.nato.int/articles/acts-delivers-texas.

2 Harrison, Kathryn, and Amelia Leopold. "How Blockchain Can Help Combat Disinformation." Harvard Business Review, August 30, 2021. https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation.

accurate data and distributing it under false titles and publishers. If a piece of media fails to be validated against the blockchain, we propose the application of a digital fake news banner to notify users that a source is unvalidated. This can be applied onto news and media sites that would like to cooperate.

In addition, we would like to target election security and election confidence in volatile nations by using the already effective Ukrainian Election Task Force that was established by The Atlantic Council, Victor Pinchuk Foundation, and Transatlantic Commision on Election Integrity. The task force maintained a rapid response team that effectively monitored, evaluated, disclosed, and successfully evaded election interference.[3] We should encourage working with this task force in order to share resources, knowledge, and capabilities in NATO's best interest. In combination we can investigate the application of using blockchain technology to register and authenticate votes and voters with the goal of easing concerns about election integrity in vulnerable populations like Ukraine.

3 Helmus, Todd. "Russian Social Media Influence - Rand," n.d. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

Stream: Foxtrot

TEAM NAME: Cyberian Huskies

AUTHOR NAMES: Kathryn Wilson, Julia Bowen, Grace Johnson, Dylan Watson

AFFILIATIONS: University of Texas at San Antonio

SUMMARY: The NATO Disinformation Collaboration Task Force of experts is responsible for aiding in the response to disinformation threats.

PITCH: In order to aid states in assessing disinformation risks as it relates to cyberspace, we propose the creation of the NATO Disinformation Collaboration Task Force. This Task Force will be composed of NATO experts, industry partners, and state representatives. Their responsibilities will be as follows:

1. The Task Force will be charged with assisting nation-states in decision-making processes in response to disinformation threats. Members of the Task Force will provide their expertise to aid in mitigation efforts by consolidating a comprehensive plan of action to address the incident.

2. The Task Force will be charged with assigning Threat Levels to ongoing disinformation campaigns. The NATO Disinformation Alert Standard will consist of four different levels. Each level indicates the available resources that can be deployed to address an individual disinformation campaign contingent on the severity of the threat. As the severity increases, the resources available will be compounded.

- Threat Level Zero will be assigned to baseline disinformation campaigns. At this level, NATO will be available for monitoring the threat per state request.
- Threat Level One will be assigned to corporate disinformation. Corporate disinformation campaigns can be defined as disinformation with the intent to cause economic harm. At this level, NATO will be available for consolidating fact-checking reports.
- Threat Level Two will be assigned to government disinformation. This can be defined as attacks on government representatives. At this level, NATO will be available for addressing the disinformation indicators. This response can include attribution discovery, the development of a counter-disinformation campaign, and other formal mitigation techniques.
- Threat Level Three will be assigned to electoral disinformation. Electoral disinformation can be defined as disinformation that undermines democratic processes. At this level, NATO will be available to host a public forum. This public forum will provide a platform to fact-check and provide transparency on the issue itself.

3. The Task Force will be charged with developing and maintaining the Disinformation Threat Intelligence Feed. This Intelligence Feed is a heat map that will be used to track active disinformation campaigns. The Disinformation Threat Intelligence Feed is populated with data curated by trained members of the NATO Disinformation Collaboration Task Force. The data is collected by processing information posted both on the internet and in other media such as television. This feed will support states in monitoring various disinformation campaigns as they occur.

To monitor performance and promote transparency, annual reports will be released on the activities of the Task Force. These reports will include performance metrics such as Time to Detect (TTD), Time to Respond (TTR), and the perceived effectiveness level as determined by member nation-states. The report will also list best practises in countering disinformation campaigns and an overview of the most prevalent attacks over the past year and how they were combatted.

The proposed Task Force will receive funding from participating nation-states. The costs will include facilities, payment for Task Force employees, and resources for the Threat Intelligence Feed. Participating nations will receive a return value on their investment by preventing economic loss due to disinformation campaigns.

We propose a NATO Disinformation Task Force that values transparency to maintain the national sovereignty of NATO member states while accounting for varying state capacities to combat disinformation. The proposed Task Force and its responsibilities will strengthen NATO and participating nation's ability to counter disinformation by increasing cyberspace situational awareness. Such steps are essential for protecting the liberal world order in the digital domain.

Stream: Golf

TEAM NAME: International Strategic Capacity Council

AUTHOR NAMES: Alexandra Hardwicke, Emila Connolly, Monica Virk, Chloe Chan

AFFILIATIONS: University of Calgary

SUMMARY: The implementation of a specialised NATO council to be in reliable operation that deals with reports from member states about threats of disinformation during times of vulnerability and polarisation.

PITCH:

Article I:

As social platforms are being used as a weapon, our campaign acts to utilise it as a tool to promote cyber security through education and transparency. To combat disinformation, we propose the implementation of a specialised NATO Strategic Cyber Security Council alongside legislation in a 12-month probationary period. The council will be in constant operation and will deal specifically with reports from the member states regarding threats of disinformation during times of vulnerability and polarisation. The council will operate within NATO's Cyberspace Operations Centre. The council will be subject to the following accountability measures:

- Five to nine members on the council that represent designated regions, with staggered five-year terms
- It must be a non-partisan independent body, free from overarching pressures or influences
- Delegates are selected from various member states based on qualifications
- They will decide on an action plan on a case-by-case basis. We estimate that the starting budget for the council will require 3% of the NATO Security Investment Program which is approximately US $21.3 million. It will primarily be funded through joint contributions among member states.[4]

Article II:

The objective of this council is to be able to exercise a level of discretion in regards to the reports through a set of qualifying criteria that is necessary for submission. Often international councils and committees are bogged down by mass amounts of information and reports that may or may not have pressing objectives that need to be addressed immediately. As a solution, we propose a criteria for disinformation reports including the following:

4 NATO, "Funding NATO," NATO, June 11, (2018), https://www.nato.int/cps/en/natohq/topics_67655.htm?selectedLocale=en .

- The threat must be directed at or prohibits the functionality of public safety
- The threat's scope has the potential to go beyond the cyber world
- Proof of external state interference
- Heightened state vulnerability (i.e.: during elections or referendums)
- Polarisation on societally significant matters

The following criteria was inspired by recent disinformation attacks and the impact such attacks had on select countries' societies.

Article III:
Following the probationary period we plan to introduce disinformation legislation. The council will draft legislation that mirrors the NATO's Smart Defence Clause which requires member states to implement cyber security systems that flag algorithms that reproduce content that is deemed as "purposely misleading" or "concerning."[5] These systems are designed to validate or invalidate content. States will be required to formulate bot control by limiting account creations per IP address or by other traceable means. In the advent of the creation of the task force, member states will support the pursuit of collective security by providing appropriate infrastructure for cyber defence. This initiative will be expressed in two ways: transparency initiative and digital literacy initiative.

Article IV:
In conjunction with the probationary period, NATO will create publicly available resources on digital literacy for educators and other interested parties to access. Member states will be required to develop a digital literary program that is funded by each country's government. Digital literacy is key to having an engaged and well-informed citizenry that is more resilient to disinformation.[6] Each member country will be required to create and maintain an online reporting system for civilian concerns.

Moving forward, the council will release publicly available reports on potential disinformation threats and attacks, with a focus on vulnerable state-statuses. The council will subsidise ads on highly trafficked social media sites. These ads will target vulnerable communities most susceptible to disinformation and provide digital literacy reminders. Finally, one delegate from the council will maintain a relationship with companies like Facebook and Google, to keep an open line of communication between NATO, the private sector, and the public.

---

5 Efthymiopoulos, Marios Panagiotis. "A Cyber-Security Framework for Development, Defense and Innovation at NATO." Journal of Innovation and Entrepreneurship 8, no. 1 (2019): 1–26. https://doi.org/10.1186/s13731-019-0105-z.

6 Hall, Holly Kathleen. "The New Voice of America: Countering Foreign Propaganda and Disinformation Act." First Amendment Studies 51, no. 2 (2017): 49–61. https://doi.org/10.1080/21689725.2017.1349618.

REFERENCES

Efthymiopoulos, M. (2019). "A Cyber-Security Framework for Development, Defense and Innovation at NATO." Journal of Innovation and Entrepreneurship 8, no. 1: 1–26. https://doi.org/10.1186/s13731-019-0105-z.

Hall, H. (2017) "The New Voice of America: Countering Foreign Propaganda and Disinformation Act." First Amendment Studies 51, no. 2: 49–61. https://doi.org/10.1080/21689725.2017.1349618.

Harrison, K. and Leopold, A (2020) "How Blockchain Can Help Combat Disinformation." Harvard Business Review, 30th August 30. https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation.

Helmus, T. "Russian Social Media Influence - Rand," n.d. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

NATO. (2018) "Funding NATO." 11th June, https://www.nato.int/cps/en/natohq/topics_67655.htm?selectedLocale=en

NATO. (2020) 'ACT's Agile Process Delivers TEXAS Ahead of Schedule: NATO's ACT, 18th September. https://www.act.nato.int/articles/acts-delivers-texas.

PART IV:
Other Pitches

All Pitches

Stream: Alpha

TEAM NAME: Cyber Eagles

AUTHOR NAMES: Owen McManus, Hope Hageman, Marshall Ney, Elijah Jeffries

AFFILIATION: Ashland University

PITCH: The most effective plan of action we can take is to improve media literacy. There is no form of censorship that is adequate to stop these cyber attacks while still allowing for a free and open society. Instead, NATO should create a set of standards for media literacy which protects society while allowing flexibility for member states to achieve these goals. Ultimately, it is up to the common folk of NATO countries to use better judgment online when dealing with scams, phishing attacks, and disinformation campaigns. Thankfully, NATO can assist our citizens and allow us to rely on the good and wise nature of people in general. No matter how compelling of a story the trolls can create, the truths of our liberal societies will eventually win in the hearts and minds of our peoples. We just need to give them a nudge.

TEAM NAME: Attack on Owls

AUTHOR NAMES: Amy Guan, Lavender Jin, Jess Wang

AFFILIATIONS: Bryn Mawr College

PITCH: We aim to combat disinformation through three actions. Firstly, we would like to raise public awareness by popularising the idea of disinformation through NATO websites and providing related authorised educational resources. This enables the educated public to identify disinformation and decreases their possibility of being misled by disinformation.

Secondly, we would like to coordinate with social media to provide page warnings that show up on sensitive topics that might mislead people and weak areas where seditious posts and comments are made.

Thirdly, we would utilise the current NATO platforms such as Instagram or Twitter to provide original information to users. NATO could conduct online live interviews on these platforms by inviting individual politicians or campaign parties or inviting third-party editors by reviewing politicians' statements to ensure the originality of the information released to the public.

TEAM NAME: ODU Fedora Fellows

AUTHOR NAMES: Kayla Macpherson, Hector Gomez, Elijah Gartrell, Brandon Zakaras, Sandon Brent, Jeremiah Price

AFFILIATIONS: Old Dominion University

PITCH: With the guidance of the UNESCO handbook and NATO associated countries such as Estonia and Finland as starting points for beta trials, NATO News could become a reality in the next calendar year. Being rooted in the desire of providing accessible, honest information for learning purposes, building a community of learners searching for answers will not only build trust with our news source, but with NATO as a whole. We understand the threat that disinformation presents for ourselves, our governments, and our future. Allowing the younger generations to help drive the change in the world they are soon to take on is simply responding to their demands and desires. We understand the fears that the world has in the current media, and we wish to absolve them. Truth is not subjective, and we are ready to prove that.

TEAM NAME: Banana Pie

AUTHOR NAMES: Jean-Pasqual Sindermann, Laura Kälberer, Anna-Feliz Sindermann

AFFILIATIONS: Old Technische Universität Berlin; Humboldt Universität Berlin; University of St Andrews

PITCH: Bearing in mind the importance of freedom of speech and without wanting to restrict people's access to and use of social media, our solution to the problem of disinformation within social media is the following: NATO develops an algorithm to detect possible trending topics. For these topics, NATO will do a preliminary fact-check and publish a website containing both facts and disinformation being spread about that topic (showing why it is

false). It will cooperate with private companies such as Facebook, Twitter, and Instagram, to insert a disclaimer visible for every post falling under that topfic, that will inform people about the website and where to find more official information.

TEAM NAME: Cyberguards

AUTHOR NAMES: Gamze Kandemir, Abdul Moiz, Jadyra Akhmukhanova

AFFILIATIONS: Antalya Bilim University

PITCH: How can NATO enhance cybersecurity awareness and readiness in order to combat disinformation online in particular on social media where the threat is constantly evolving?

The case study brings up the problems which are currently being faced globally, i.e., Europe. In the solutions given below, we have used different tactics to tackle with what is known to be the assurance of sovereign freedom and to get rid of threats the international community is fronting through cyber security issues. A proposal of fact check is being put up on both micro and macro level where there will be a formation of an association run by professionals from different fields of expertise such as academicians, military personnel, activists, and bureaucrats, etc. In addition, with that we are proposing to have a Stock Mechanism for the information flow among the borders to create transparency and ability to deal with unexpected threats effectively.

TEAM NAME: Final 3

AUTHOR NAMES: Jason (Qihao) Yang, Jane (Jingzhi) Zhao, Haley Chen

AFFILIATIONS: William & Mary

PITCH: Different cybersecurity laws in each country cause difficulties with implementing international law and cooperation. Some countries are unwilling to cooperate for economic or political reasons, causing information gaps. Based on the issue identified, we propose two solutions: setting up international platforms and fostering activist groups.

By setting up international cyber platforms, we can provide major resources and opportunities for information access. Specifically, we could lessen wrong information by establishing a global cyber platform with professional regulation teams. These teams consist of experts from various backgrounds to restore facts through independent evaluation.

By fostering informed activist groups, we could encourage more valid government regulations for disinformation. The cyber platform could provide help and education to activist groups from law and cybersecurity professionals. Thus, activists can obtain accurate and holistic information to push for constructive media laws (e.g. media licensing) that allow the government to regulate and reduce false remarks.

TEAM NAME: Article 5

AUTHOR NAMES: Ben Wheaton, Jawad Salah, Oren Abraham Keller, Luke Tonkinson

AFFILIATIONS: Cardiff University

PITCH: This action plan is a twin-pronged approach to combating cyber threats around the world. By focusing on educating the populace, through a NATO founded non-profit, we can ensure that there is an international resilience to cyber threats. The global reach of this will expand on the CTCL mechanism that has shown to be effective in the USA, which has assisted 76 million people in the US since it was founded. Further, by using the resources and capabilities of NATO diplomatically, we can pressure governments to follow the approach of Estonia, which is enforcing mandatory cybersecurity education in schools, beginning 2022. The benefits of this are self-explanatory, and go hand-in-hand with the non-profit's goals. These approaches together will help protect the international community from disinformation, and other cyber threats.

Stream: Bravo

TEAM NAME: Cyber Blazers

AUTHOR NAMES: Paige Langmead, Derek Wyld, Julian Urban

AFFILIATIONS: Hood College

PITCH: We want NATO to take action in creating a new branch to manage and control the spread of disinformation on social media platforms. This branch will be modeled off of the already existing approach of NATO's response to the spread of misinformation regarding COVID-19. We will use the understand and engage functions to analyse information and take action if needed. This committee can be built off of this model and expanded in order to meet the needs of current situations around the world. Social media plays an extremely large role in how today's news in perceived. We want to reach out to social media platforms and ensure that they are proactive in flagging misinformation in posts. We also want to be sure that we are not wasting time on posts that have an immensely low following and reach due to the overwhelming spread of false information from larger accounts.

TEAM NAME: Sparring Partner

AUTHOR NAMES: Paige Langmead, Derek Wyld, Julian Urban

AFFILIATIONS: George Mason University

PITCH: From the outset NATO should identify high-risk events within the alliance, such as elections, that are vulnerable to foreign sponsored misinformation campaigns. NATO should then support member states by increasing members' personnel capacity to counter those campaigns through deployment of specialists like linguists. We propose creation of a task force to respond to support requests from NATO members. Protecting the upcoming French presidential election can be the launch of a pilot program.

Second, NATO must enhance its partnership with the private sector, including major tech companies. In cooperation with them, we propose creation of a limited intelligence sharing mechanism where NATO can flag coordinated interference operations. In return, tech companies should disrupt those operations on their platforms.

Finally, the alliance should discourage foreign interference by increasing the cost for non-state actors involved. Those actors can include private compa-

nies that knowingly have assisted our adversaries in their operations against NATO members.

TEAM NAME: California Maritime Academy

AUTHOR NAMES: Kyle Yamamoto, Aidan Kenny, Nolan Bronstrup, Reilly Corner, Joseph Claytor

AFFILIATIONS: California Maritime Academy

PITCH: Within the realm of cyberspace, there are various challenges that are present. Within the case, an immediate challenge we identified was how to combat disinformation, which would make the strategic objective to combat disinformation, as disinformation hinders NATO and its allies' ability to deal with cyberthreats.

Within a phased approach, the first phase that we would recommend ad campaigns to be done by NATO and to encourage major social media companies to spread awareness on misinformation.

Phase two will be the establishment of the Disinformation Combat Centre or DCC (Centre de lutte contre la désinformation). This will be a NATO funded open-source intelligence centre tasked with sharing information on disinformation campaigns. DCC will partner with institutions such as the CCDCOE to share intelligence. This is a multi-year objective to develop. It will be the first of other NATO Fusion Centres tackling other aspects of Cyber Conflicts.

TEAM NAME: SUper Tar Heels

AUTHOR NAMES: Jing Xue, Wenqiong Hu, Haoran Yang, Yujun Ming, Jiayi Xu

AFFILIATIONS: University of North Carolina - Chapel Hill

PITCH: First, to resolve the problem of disinformation, we encourage politicians and their team members to verify with their real names. For accounts without real-name verification, There would be a restriction for the content which include specific words.

Secondly, we would build a machine learning model within three months to detect fake news instead of the traditional way of detecting fake news, it detects real news. If an article is written in a similar way to a real news article, so if the score comes back really low, it might mean the article is fake, an

opinion piece, or something other than a straightforward, facts-only news article.

Lastly, by using the TfidfVectorizer, we could identify the Term Frequency or the Inverse Document Frequency. Then we could read the data into a Data-Frame and build a model to accurately classify a piece of news as REAL or FAKE.

TEAM NAME: GOGOGOGO FOR IT

AUTHOR NAMES: Yuze Lang, Quanhan Zhou, Xiwen Liu, Jingwen Hu

AFFILIATIONS: William & Mary

PITCH: We found that today's problem is twofold, concerning the community and the overall environment. Specifically, we propose one program for each. Our education program first aims at enhancing college students' abilities of anticipating and discerning disinformation.We develop a web that provides online courses on identification and coping strategies of disinformation and an app for group support and discussion. After targeting college students at first, we will expand our education program to K12 and the general public. On the other hand, we have the tri-collaboration program: incorporating private companies of social media, civic organisations with NATO political experts. Besides, we will have an honor code against disinformation, encouraging and pressuring both private companies and member countries to participate in our collaboration. Our programs' social benefits outweigh the economic expense, and we will promote cybersecurity in both the short term and long term.

TEAM NAME: goal diggers

AUTHOR NAMES: Pierre Noah, Anya Bodine-McCoy, Owain Thorp

AFFILIATIONS: University of St Andrews

PITCH: We present a three-phase plan to play offense in the battle for cybersecurity. One, increase and improve a sustainable, relevant social media presence to engage young voters to support NATO and understand the threat of misinformation. Two, use this heightened social media presence to establish a threat to attackers, and develop a task force composed of member states to make NATO the go-to source for cybersecurity information, as well as publish information for both governments and intelligence agencies in addition to common civilians. Lastly, on a more technical level, NATO should use its member states' resources to monetarily de-incentivise hacks and col-

lectively develop and apply AI technology to combat future cyberattacks by facilitating partnerships between governments and industries. Ultimately it is NATO's responsibility to use technology to create a standard across its member states and sense and detect information ahead of time so as to prevent future attacks.

Stream: Charlie

TEAM NAME: Vacilando

AUTHOR NAMES: Deniz Özyurt, Eren Yekta Oyucu, Öykü Kurun, Doruk Beyazpınar

AFFILIATIONS: Middle East Technical University

PITCH: A proactive approach to solving the disinformation problem will be more effective in combating disinformation, for which we have created a three-fold project.

First, NATO will cooperate with social media companies Meta, Twitter, and Google to supplement algorithms which filter out disinformation. Considering the fact that these companies already have similar projects underway, this is meant to further develop and integrate these systems. Moreover, this will create a foundation for the second part.

The second stage is the creation of a ranking mechanism for social media users with the objective of incentivising them to proactively identify and report disinformation. Not only will this educate the masses but it will also aid in developing the machine-learning of the algorithm mentioned in the first part.

Finally, NATO will create an interactive game with the aim of not only illustrating the potential ramifications of uncontrolled disinformation but also educating the players.

TEAM NAME: Pandas - GMU

AUTHOR NAMES: Abdallah Ali, Yara Hussein, Nihaal Prasad, Zaria Shields, Tenzin Tsering

AFFILIATIONS: George Mason University

PITCH: Because the threat of disinformation is constantly evolving, the Disinformation Defence Initiative (DDI) aims to promote digital literacy in NATO countries. DDI aims to neutralise the rise and spread of disinformation in NATO countries by pursuing a vision to create and sustain a new generation of highly qualified individuals alongside the development of comprehensive computer disinformation detection algorithms.

Implementation of this framework alongside the development of necessary infrastructure is imperative to the security of NATO member countries. The

importance of collaboration cannot be stated enough, which is why the DDI will serve as a central method for NATO countries to communicate with one another on the issue of disinformation. Recognising that disinformation peaks during election cycles, our framework is to be implemented continuously post-elections to sustain the literacy environment that it will generate as well as help to diminish the evolving capabilities of disinformation centres.

TEAM NAME: Pepperdine University

AUTHOR NAMES: Haley Brouwer, Tamie Daniels, Carter Lentz, Alexis Olmstead

AFFILIATIONS: Pepperdine University

PITCH: Recognising NATO's mission to guarantee freedom and security, our team advocates for implementing the TTT Plan - Technology, Transition, Trust.

In order to promote transparency and accountability, NATO should prioritise collaboration with civil society organisations like AlgoTransparency, creating technological safeguards against disinformation that provide sustainable and cost-efficient solutions over the next several decades, as these safeguards can be re-implemented for various scenarios such as the Ukraine election.

As cyber-life becomes more intertwined with human reality, the successful connection between technological reforms and credible, trustworthy relationships becomes increasingly important. Through partnerships with independent, multicultural individuals and experts, NATO can cost-effectively create a coalition of fact-checking parties to actively fight against disinformation.

Lastly, our plan seeks to foster trust within the realm of cybersecurity by curating informational resources and making them readily available to local communities within national globally to bolster public safety campaigns that are adjustable to various audiences.

TEAM NAME: KCL-HUMINT

AUTHOR NAMES: Lilla Doucha, Ariel Koh Min, Dorottya Zsiboracs

AFFILIATIONS: King's College London

PITCH: Building on the democratic deficit following Russian disinformation campaigns in Ukraine, we propose a multidimensional strategy focused on 3Cs: Cementing resilience–widening awareness in the long run towards disinformation campaigns; Common vision–protecting democratic values to prevent disinformation from fragmenting NATO unity; and Cooperation–between stakeholders to guard against information operations. This strategy enhances NATO efforts, utilising educational tools targeted at societies and the military, technology to filter coercive content and bolstering diversity in NATO's strategic communications department to include underrepresented voices to Cement resilience. To build a Common vision, we suggest bolstering NATO influence in countries least supportive of NATO to firstly safeguard NATO values. For Cooperation, this touches upon establishing code of conducts between NATO and private sectors and for users, cyber-norms within NATO, for academic linkages to be deepened and to enhance visibility of present efforts like the NATO Innovation Hub to include greater whole-of-society cooperation.

TEAM NAME: Blue Team

AUTHOR NAMES: Bradley Berklich, Owen Fitzgerald, Zach Sclar, Delaney Gallagher

AFFILIATIONS: Kenyon College

PITCH: Barrier nations such as the Ukraine, Moldova, and Georgia are subject to outside interference through social media. NATO can counteract these plots, but it needs to cultivate trust and establish legitimacy within these countries. Our three-pronged approach entails creating a new agency dedicated to open source collaboration, of which one tool it will provide is a 2SV measure in order to track IPs of bad actors and make bot accounts less feasible. On the ground, the civil team will work, live, and recruit from the local community in an anticipatory effort to promote trust between the general populace and NATO, and to preserve social cohesion and stability, all while allowing them access to NATO resources After identification, the third prong, INTERPOL, will be relied upon to subdue bad actors, return resources to local governments, and disrupt echo-chamber algorithms with neutral information administered in cooperation with local governments and NATO.

TEAM NAME: Disinformation Destroyers

AUTHOR NAMES: Joshua Murray, Redeit Hailu, Lilly Doninger, Laura Lam

AFFILIATIONS: William & Mary

PITCH: Lack of communication among NATO member states on disinformation contributes to insecurity and instability of global democracies. Our bottom up approach (CFIL) with a Khan Academy Sponsored Education Program addresses public awareness and misinformation prevention. Additionally our top down approach (AVIS) addresses readiness through a communicative alerting channel. A conglomeration of NATO Member States, private social media companies, and NATO sponsored detection and alert teams will collaborate to identify and report misinformation that is being released and facilitate reciprocal information flow. Detection and alert systems will be based on preexisting technologies. We understand that disinformation is an ever-present and ever-growing concern, so we believe both a long term and more immediate solution is necessary. Lastly, the joint CFIL and AVIS solution is scalable beyond NATO in the future.

TEAM NAME: j2k

AUTHOR NAMES: Katherine Hughes, Kayleigh Robic, Jack Bratton

AFFILIATIONS: University of St. Andrews and William & Mary Joint Degree Programme

PITCH: NATO is currently facing disinformation threats from actors both external and internal. NATO should humorously expose bad actors on social media. This will help NATO connect with younger audiences and demonstrate how to identify disinformation. NATO should engage in pre-planning and pre-engaging with local communities at acute risk for disinformation operations. NATO should work with local, trusted figures to highlight the presence of disinformation. NATO should clarify Article 5's stance on cyberattacks and disinformation, to empower NATO to respond. Also, NATO should use existing institutions to change policies regarding internal management to allow for countermeasures directed at NATO member disinformation against fellow members. This solution includes difficult, but necessary structural reforms, as well as engagement with populations most at risk. Without these changes, NATO will remain susceptible to disinformation and threats in cyberspace.

Stream: Delta

TEAM NAME: NAK Associates

AUTHOR NAMES: Kirill Usubyan, Alex Kolar, Noah Schulman, Sydney Smith

AFFILIATIONS: William & Mary

PITCH: Within the NATO Communications and Information Agency, a new task force will be created called the Disinformation Task Force. This group will develop a simple user-friendly game that teaches social media users how to identify misinformation. This game will be incorporated into social media registration processes and made a requirement for existing users. The game will be periodically updated with the addition of special event prizes during peak times of disinformation spread. As users grow more accustomed to identifying disinformation, the developers will create more difficult stages of the game, and players will have an opportunity to be on a network wide leaderboard indicating their prowess in identifying disinformation. This leaderboard may be useful to NATO, as it will provide a list of informed citizens. This approach appeases private companies by giving them a way to visibly show their concern while avoiding any changes in the algorithms that made these sites popular.

TEAM NAME: Canadian Computer Scientists

AUTHOR NAMES: Alexandra Tenney, Jeremy Stuart, Yasmin Samantar, Delara Shamanian

AFFILIATIONS: University of Calgary

PITCH: Our solution would be to create a NATO Media Analysis Centre to scrape publicly available social media posts for storage and analysis. This centre will implement an analysis program that will analyse for influence, engagement, and shares to identify the most influential posts and users. Humans will then sort through these posts and identify misinformation and disinformation. This will be fed back into the system to track these users and trigger an alert when their posts reach a sufficient level of shares/influence, and NATO will craft messages to counter the disinformation.

NATO must then make this analysis publicly available and work closely with local media sources in member countries to share the story of the disinformation and the corrected information. The media relations office of NATO must be more than just an organisation that responds to the media and proactively engage them, specifically on disinformation.

TEAM NAME: Hamilton College Continentals

AUTHOR NAMES: Peter Huleatt, Eric Jamous, Jonathan Gerstein, Joe Largo

AFFILIATIONS: Hamilton College

PITCH: A lack of digital literacy makes people particularly vulnerable to disinformation. Fact-checking, content removal and damage control cannot address the full amount of disinformation in the information ecosystem. A two-pronged, grassroots-driven approach consisting of disinformation training and a user-generated ad repository can mitigate the problems posed by disinformation at a low cost. Disinformation trainings will increase user's knowledge and awareness of disinformation so they are better able to identify it, and less likely to fall victim to it. Once they have completed training, users can submit screenshots and other relevant information of advertisements they see on social media. This creates a repository of advertisements, bursting the filter bubble and providing NATO and social media companies with situational awareness as they get a sense of the size, scale, and scope of disinformation. User participation is incentivised through a token-based reward system.

TEAM NAME: Baylor Cybears

AUTHOR NAMES: Jack Beckis, Austin Gould, Jose Arraiz-Rada, Alejandro Navarro, Miranda Montroy

AFFILIATIONS: Baylor University

PITCH: Private social media companies such as Facebook and Twitter have a political disinformation problem and are looking for a solution yet may be reluctant to allow governments to manage their platforms. NATO can act as a third-party authority with the human resources necessary to combat social media disinformation. NATO could independently "fact check" posts and accounts suspected of spreading disinformation. This would allow information to be verified by an unbiased third party that users can trust, reducing biased fact checking. NATO can then label posts as "Suspected Disinformation", "Verified by NATO", or "Unchecked by NATO." This process of labeling disinformation yet not censoring is important for transparency. Furthermore, NATO could contact individuals who engage with a certain threshold of labeled "disinformation" with information regarding the background of certain political misinformation. Finally, NATO could introduce anti-disinformation bots that can flood channels of disinformation with information regarding the background of political disinformation.

TEAM NAME: St Andrews Office of External Affairs

AUTHOR NAMES: Michael Schmitz, Nadezhda Kitipova, Elise Murphy

AFFILIATIONS: University of St Andrews

PITCH: The action plan aims to enhance the situational awareness and readiness of NATOs efforts to combat disinformation and election interference. Although cyberspace was recognised as one of the key domains of NATO's structure, it is currently not treated as equally important to the other three: land, maritime and air. At the moment, it is the responsibility of the targeted state themselves to combat any cyber threat, rather than it being considered a collective security issue, despite being classified as such. The NATO Industry Cyber Partnership is an already existing framework that could be used to incorporate key companies such as META through incentivising their cooperation. This could be used to also extend the functions of the Cyber Rapid Reaction teams to act on a regular basis and not per request. Thus, using ethnic awareness disinformation in the run ups to key events could be combated through targeted information campaigns.

TEAM NAME: Keele Squirrels

AUTHOR NAMES: Jack Houghton, Polly Sutherland, Christian Recchia, Arjun Sinha, Oliver Levitt-Allen

AFFILIATIONS: Keele University

PITCH: The creation of NATO-ADAC (NATO Anti-Disinformation and Cybercrime) which would facilitate a comprehensive media and resource campaign across all major social media websites, raising awareness of actions that hostile actors use online to endanger democracy, freedom, and truth through disinformation and dangerous cyber activity.

In collaboration with industry leaders in the technology sector, domestic governments, and local leaders, NATO-ADAC would publish informational content and campaigns through various legitimate sources at times when manipulation can be seen, aiming to target those vulnerable before maligning actors have a chance to disrupt the online public sphere. Campaigns could include #CheckThisForMe, a tool used by the public to mark content that could be harmful, which would then be either factchecked by the community or sent to respective cybersecurity agencies for analysis. In doing so, placing the onus on public to be aware of risks and to encourage healthy legitimate participation when online.

Stream: Echo

TEAM NAME: NATO field School - SFU

AUTHOR NAMES: Jack Burnham, Caterina Fusco, Samuel Nadeau, Adelaide Scott, Carmen Hui

AFFILIATIONS: Simon Fraser University; University of Western Ontario; Queen's University

PITCH: Two-pronged approach using social-political response with a technical component that combines computer algorithms and human intelligence. Our project scans and identifies information/trends/keywords/events and issues relevant to the Alliance, seeking out disinformation in order to analyse and disseminate trends and recommend policy approach

This approach will utilise NATO's strengths in interoperability, human capabilities, and multilateral approach by relying on NATO's edge in technology and expertise and broad sources of knowledge and seeks to make NATO more active and transparent by sharing the results of its analysis with public outlets. The feasibility of this approach is within the means and capabilities of NATO, utilising existing technologies and resources that can be implemented within the calendar year.

We have chosen Latvia and Estonia as framework nations to provide leadership and training, other NATO nations will follow. The human component will ensure close monitoring of changes in trends that will aid in informing the technical component

TEAM NAME: Magenta Commandos

AUTHOR NAMES: Lucas M. Kisabeth, Donnis D. Kent, Shane M. Iams, Dylan M. Hissner, Reilee E. Gillman

AFFILIATIONS: Muskingum University

PITCH: Stopping the spread of misinformation is a nearly impossible task. Our solution recognises this and instead focuses on combating misinformation with facts. Our dashboard will visualise the scale of misinformation across the globe both broadly and specifically. Social pressure by the general public will force Big Tech as well as Governments to recognise the results of the dashboard and act accordingly. The project should be open source in order to be as transparent as possible, as the goal of the dashboard is to be unbiased and truthful. Financially, the project is affordable. Most costs would stem from the initial creation of the website and necessary API. There would

be costs associated with building a data science team and maintaining the site. Trends in the data overtime would reveal the efficacy of the solution. It can serve as a platform upon which other innovations can be built.

TEAM NAME: ZBD Thinkers

AUTHOR NAMES: Piotr Wierzbicki, Joanna Szuberska, Antonina Kotlarz, Anna Hartman

AFFILIATIONS: University of Warsaw

PITCH: This project proposes Prevention, Prediction, and Counteraction as a solution to the case concerning disinformation in social media. Prevention is understood as reaching out to common users by publishing articles about disinformation and offering free trainings on the topic. Prediction is about an implementation of AI in order to help analytical teams detect conflicts on time. Last but not least, Counteraction is about sending alert signals about possible disinformation while maintaining full transparency in actions. In conclusion, the PPC method should not only successfully spread awareness, thus educate social media users, but also reduce future disinformation online.

TEAM NAME: East Shore's Best

AUTHOR NAMES: Lucy Hope, Emma Downey, Campbell MacPherson

AFFILIATIONS: University of St Andrews

PITCH: Aim to set up a centre with the focus of monitoring public media and countering identified disinformation as well as being actively involved in circulating corrected information during upcoming elections of NATO States:

- Focusing on election periods narrows the scope the unit to the most sensitive times during which disinformation may be spread
- Acting as a resource available for NATO Member States in time of need rather than automatically tackling the circulation of disinformation
- Focusing on monitoring public media rather than the spread of private information, keeping in consideration legal privacy requirements
- Collaborating with stakeholders who are trusted and influential in the regions at hand to gain public trust and account for regional media differences.

TEAM NAME: Possible Poker

AUTHOR NAMES: Jacques Worth, Aaron Tavel, Chris Mize, Gabe Dakake, Wyatt Biddle

AFFILIATIONS: William & Mary

PITCH: First, NATO should focus on implementing an education plan to raise awareness in Ukraine of the existence and signs of disinformation in the news and social media. Within schools, NATO will work to infuse critical thinking and research methods within each core subject to highlight specific areas in which disinformation is prevalent. This will prove to be both feasible and sustainable as students will understand and continue to learn about disinformation which will create a more mature and free-thinking online community.

Furthermore, NATO will expand their social media presence, working alongside nonprofits, in order to combat the spread of misinformation in Ukraine. This includes buying Facebook ads to provide the general public with educational information regarding cyberspace security and disinformation, specifically within politics. While the educational plan targets the younger generation, a larger social media presence will allow NATO to educate adults.

Stream: Foxtrot

TEAM NAME: Defenders of the Sample Gates

AUTHOR NAMES: Clayton Greis, Shanay Shah, Gabriel Burdeen, Max Krajacic

AFFILIATIONS: Indiana University

PITCH: NATO can maximise cyberspace awareness and readiness to combat disinformation through the utilisation of the Observe-Orient-Decision-Act loop as a decision-making heuristic framework. Our solution creates robust observation capabilities through the consolidation of cyber and public relations units into a single Disinformation Command. Partnership with private technology companies is critical to orienting towards emerging and evolving cyber threats. Utilising the NATO Industry Cyber Partnership, NATO can analyse disinformation using natural language processing and predictive analysis in partnership with private firms to create a responsive decision-making loop. Decision points analytically created by this responsive loop can be used by Disinformation Command to decide on the best courses of action. In final action, Disinformation Command can operationalise effective responses and then provide predictive analysis reports to private technology partners to enhance further response capabilities on emerging disinformation threats.

TEAM NAME: Dokuz Eylül

AUTHOR NAMES: Abdulkadir Mücahid Ünsal, Bilgehan Katipoğlu, Ceyhun Tutar, Mert Güven, Zeynep Elif Turgut

AFFILIATIONS: Dokuz Eylül University

PITCH: This project will require many specialists and skilled engineers; they will be active on the internet and develop a machine learning system to increase effectiveness. This software will develop as a form of mobile application. It will collect data from social media platforms and will provide fact-check mechanism. The social media users may share their intended information with the app and can compare it with data and have certain percentage for correctness. The app system focuses on certain keywords in social media and official news websites. The app will function during the election campaigns to reduce political tension, polarisation, and spreading of disinformation. Budget of this app come from member states and voters donations. Because disinformation triggers member states security concerns and voters can be encouraged with the security of their votes. So we can fund the developers of the software and cyber-security team that control the rule of the application.

TEAM NAME: Soldiers of Troy

AUTHOR NAMES: Rhiston Yu, Luke Wilson, Nathan Hyun, Vaneet Saini

AFFILIATIONS: University of Southern California

PITCH: In order to counter the rise of digital disinformation and propaganda campaigns, we propose NATO develop a working group or task force that builds on the framework of the Global Internet Forum to Counter Terrorism (GIFCT) and the U.S. State Department's Global Engagement Center. This working group will build upon this existing civil-government-military relationship to identify, understand, and counter disinformation and propaganda efforts by state and non-state actors. It will create a hash database of disinformation and propaganda content for use by governments and corporations to curb disinformation campaigns and prevent its amplification. This database will also build a profile of state and non-state actor groups to help with identifying and understanding of their methodology and characteristics.

TEAM NAME: Aqua Sleuths

AUTHOR NAMES: Conor Sokolowsky, Noah Fields, John O'Hara

AFFILIATIONS: William & Mary

PITCH: Cyber warfare is a constantly evolving battle ground where civilians are the pawns of disinformation schemes led by opponents like Russia. Our plan consists of 2 components. First is a database containing all relevant campaign information submitted by verified candidates organised and maintained by NATO that is accessible to all countries under the threat of being meddled with. Second is a course that trains people how to recognise fake articles and report them to be verified. This course would turn into a game where players can level up by watching more lessons and correctly identifying fake news. This course should be accessible on all platforms, in all languages. Hopefully social media companies would partner with NATO and remove articles that are reported.

This is a very scalable and sustainable solution that can adapt to the future of cyber-warfare. The educational component is also a valuable long-term investment.

TEAM NAME: ELAIM

AUTHOR NAMES: Emmanuella Taiwo, Maria Gaggino, Isabel Perojo Arroyo, Leo Shoebridge, Alex Jacklin

AFFILIATIONS: Nottingham Trent University

PITCH: A plan to implement a verification system in which a three-tier verification on social media platforms, a circle verification ring will appear around the individual's picture. This verification is here as a reliability symbol to other users and therefore, individuals posting online are exposed to other users if they are not verified by a social media account and individuals that see the post can be aware that this post may not be true or a reliable source. Furthermore, within the election period of a NATO member state, social media companies will tag any posts that contain key words (e.g., *country* election) being with a link to a NATO run website that includes information on the election such as candidate manifestos, debates, etc. This tag will simply give people the option to research the post and link attached to stop any misinformation being spread like social media companies do with COVID-19.

TEAM NAME: Seawolves

AUTHOR NAMES: Justin Chan, Bryan Kormendi, Taulant Rama

AFFILIATIONS: Stony Brook University

PITCH: If NATO countries are to successively combat disinformation, they must regulate social media companies like they are public utilities, just like you would for a telephone or electric company, so that free speech and other enlightenment values can be expanded to cover social media platforms, which should be regarded as the new public squares. If it is not regulated as a public utility, the only alternative would be for governments to censor speech, which would in turn make the populace angry and make them more inclined to listen to disinformation and distrust their government. NATO would enforce this type of system by rewarding countries who comply with this measure. Specifically, these countries would gain greater representation in NATO decision-making than those who do not. In regards to sustainability, NATO will hold many Open Town Hall Meetings and YouTube Live Streams to educate the populace about the importance of combating disinformation. Additionally, livestreams on some internal NATO meetings would also provide more needed transparency. This would also be a very cost-efficient method.

Stream: Golf

TEAM NAME: St Andrews IR Tutorial Group 26

AUTHOR NAMES: Sai Madhav Singh, Koichi Akashi, Daniel Brathagen

AFFILIATIONS: St Andrews University

PITCH: Our fact checking social media interface utilises pre-existing NATO structures and protocols and combines them with a new innovative method of analysis and implementation. The interface would include a search tab where users are encouraged to check suspicious or polarising information and would provide them with accurate unbiased information in response. The proposed interface would be suggested in a NATO act which would recommend that individual states legislate domestic social media platforms to include an integrated fact checking interface. The interface would involve an information exchange and library which would monitor and analyse disinformation trends. Once disinformation is recorded and analysed, rapid response forces would be deployed to counteract any specific threats identified. Initially, the interface and analysation of disinformation will focus on individual national elections allowing for a scalability aspect. The interface is a comprehensive method of targeting and analysing disinformation whose target is to monitor trends not individuals.

TEAM NAME: Team JHU Cyber Attack Predictive Index

AUTHOR NAMES: Hritamber Chakraborty, Justin Limberg, Greta Maras, Emily Mehler, Chris Park

AFFILIATIONS: Johns Hopkins University

PITCH: Continually and rapidly evolving disinformation campaigns threaten NATO members and require allies to acquire nimble situational awareness (SA). We thus first recommend the creation of a NATO committee and task force that improve SA by bringing together member countries, civil society groups and organisations, and social media companies. NATO will designate countries waging disinformation warfare against NATO allies as "Disinformation Threat Actors" (DTA). Situational awareness informs our two-part readiness and resiliency-building measures (RBM): active countering and institutional countering. Active countering combats ongoing disinformation campaigns and information pollution from DTA through a competing information campaign that targets NATO citizens. Institutional countering will mitigate DTA threats through the enhancement of media literacy programs. We recommend the creation of nation-specific media literacy controls to es-

tablish an international standard of literacy. The results of the RBMs then would lead to changed disinformation campaigns and new inputs that would then inform new SA.

TEAM NAME: Soul Celestia

AUTHOR NAMES: Mehak Ghai, Grace McCartney, Stefana Velescu

AFFILIATIONS: University of Calgary

PITCH: Evolving disinformation efforts pose a challenge to NATO members, forcing them to develop innovative solutions. The creation of a council proposed by our group would utilise the effectiveness of teamwork to combat disinformation. Called the "International Strategic Council of Media and Disinformation," this council comprises NATO members, social media representatives, and third-party researchers. The council will provide global cooperation and engagement in preventing the spread of false information. Additionally, there will be engagement with social media companies by providing incentives of honour and publicity and debunking incorrect information, allowing for the control of the amount of exposed information in a set time and applying the prebunking strategy.

The team proposes the creation of "NATO Star": a set of digital "influencers" that not only will appeal to the younger generation through the online "influencer" appeal, but will also raise the 'cyber' capital of the organisation.

TEAM NAME: Otterbots

AUTHOR NAMES: Katherine Crandell, Mira Wroblewski, Leo Glikbarg, Anne Hruska, Kunal Sinha

AFFILIATIONS: Stanford University; University of Edinburgh; William & Mary

PITCH: We propose NATO take both defensive and proactive approaches to limit rising international security threats.

Defensively, establishing an annual conference exclusively on disinformation will allow member countries to: review ever-evolving cybersecurity threats, propose policies, and present reports on how they have combated threats. This will encourage members to prioritise pressing cybersecurity issues and keep research and solutions coordinated and up-to-date.

We also propose a cybersecurity task force that will expand and guide the existing NATO Counter-Hybrid support teams to work with member states

on developing digital literacy programs, reviewing and documenting content online, and ensuring fair elections.

Actively, we propose that social media companies introduce more accessible verification processes, beginning with media outlets and companies, but with an option for all individuals to also pursue official verification in the future.

These policy proposals foster active awareness around cyber threats and scale to create a more sustainable and trustworthy cyber landscape.

TEAM NAME: Hofstra University

AUTHOR NAMES: Sagarbir Bandesha, Marissa Haas, Kayleigh Specht

AFFILIATIONS: Hofstra University

PITCH: Aligning with NATO's mission to promote democratic values and enable members to cooperate on defence and security-related issues, our proposal is to further enhance member security through creating an additional page to the NATO website which will act as a hub for useful, verifiable information. With the goal to provide a neutral unbiased transparency to counter misinformation and propaganda, this information would be a source for members to attain fact checks and background information on political speeches and articles. The end goal for this NATO page addition is to host a National Media Literacy Week and Events, provide a concise list of state sponsored media sources to better apprise the people, and to provide coverage of elections and summits. This end goal allows for future advancement through partnering with social platforms to further cyber awareness. While countering disinformation is a national responsibility, Article 5 makes it NATO's responsibility to help create cyber awareness to ensure security across all members.