CCDCOE

WMGIC
GLOBAL INNOVATION CHALLENGE

WILLIAM & MARY
CHARTERED 1693

2023 WMGIC X NATO COUNTERING DISINFORMATION CHALLENGE

S. Dinesh, D. Gao, G. Hage, I. Kung, T. Lawrence, S. LoBue, B. Michael, M. Newcomb, P. Pernik, K. Rachamallu, T. Stearns, K. Whittle, S. Workinger, L. Urban, A. Vij (Eds.)

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

The NATO CCDCOE is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from the military, government, academia and industry, currently representing 39 nations. The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations and law. The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors.

Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields allows cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects. The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decisionmakers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring. 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. 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. WMGIC has received support from the Whole of Government Center of Excellence and the Reves Center for International Studies at William & Mary. To learn more about this Challenge or engage with us, contact wgc@wm.edu.

Disclaimer

The views expressed in this volume belong to the authors of the chapters. This publication is a product of the NATO CCDCOE. It does not necessarily reflect the policy or the opinion of the CCDCOE or NATO. The CCDCOE may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

2023

WMGIC X NATO

COUNTERING DISINFORMATION CHALLENGE

S. Dinesh, D. Gao, K. Floyd, G. Hage,
I. Kung, T. Lawrence, T. Longo, S. LoBue,
B. Michael, M. Newcomb, P. Pernik,
K. Rachamallu, T. Stearns, K. Whittle,
S. Workinger, L. Urban, A. Vij (Eds.)

WILLIAM & MARY
CHARTERED 1693

TABLE OF CONTENTS

LETTER FROM THE EDITORS

The NATO Alliance and Partner Nations confront a diverse range of challenges to international peace from a variety of sources. Many of these threats go unnoticed, invisible but prevalent throughout the world. Disinformation has risked the safety of individuals, nations, and the international community, spreading rapidly and unrecognized. As such, preventing its proliferation and mitigating its effects requires the efforts of individuals from all spheres of society to utilize their diverse tools and experiences.

NATO Headquarters has again partnered with William & Mary's Global Innovation Challenge (WMGIC) and Whole of Governance Center of Excellence (WGC), challenging undergraduate students from across the Alliance and Partner Nations to tackle the issue of disinformation in seven unique fields.

The fourth annual Global Disinformation Challenge brought together students from 35 teams across 16 countries on November 3, 2023 to develop innovative solutions to pressing disinformation challenges. Organized into six streams, teams confronted disinformation in Artificial Intelligence (AI), the Russia-Ukraine War, Public Health, Sexism and Gender-Based Violence (GBV), Terrorism, and Human Rights. Over the course of seven hours, teams devised solutions, advised by expert mentors in their selected topic. Each team then presented their solutions to a panel of judges who rated their proposals on the following criteria: feasibility and effectiveness, creativity, privacy, sustainability, and fiscal pragmatism. The list of distinguished mentors and judges is contained here within.

Seven winning teams were selected based on their innovative, tangible, and sustainable recommendations to NATO HQ. However, as all teams demonstrated their ability to offer creative and practical advice to NATO HQ, every team's pitch is contained in this publication. Their solutions show promise for the next generation of problem solvers and may prove applicable in current projects against disinformation. Therefore, we ask that if you include any team's solution in your work you attribute it to the team that produced it. We feel their solutions are worthy of publication, and are excited by the influence they may have on current approaches to disinformation.

We would like to thank our principle supporters, William & Mary DisInfo Lab, the Whole of Government Center of Excellence (WGC), and the Reves Center for International Studies.

Sofia LoBue
Shradha Dinesh
Dorothy Gao
Aaraj Vij

Katherine Whittle
Brennen Michael
Terra Stearns
Kiran Rachamallu

Ian Kung
Sophie Workinger
George Hage

FOREWORD

NATO recently celebrated its 75th anniversary. The Alliance exists to safeguard the freedom and security of its member states, to promote democratic values, and to create the conditions whereby member states can work together to prevent war and preserve peace. In addition to greater competition from authoritarian states, the Alliance faces other threats including cyber attacks and disinformation. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) supports the deterrence and defense of the Alliance in and through cyberspace. When we reflect on whose brain power is going to best address the latest threats involving disinformation online and on the battlefield, we can think of no better group than undergraduate students.

Under the guidance of the oldest public university in the United States, William & Mary, these bright youths came together to answer NATO's call to be creative and innovative to stop the influence of malign actors seeking to sow seeds of discontent and disrupt democratic institutions. Each team had its own approach and unique way of combating a particular aspect of disinformation, guided by what they were witnessing in Croatia, Italy, Romania, Ukraine, and more. This is the generation that intuitively understands the power of a smartphone and a deep fake, and is fast and cunning enough to blunt the impact of an information operation.

Some of the ideas contained herein could be implemented today. We hope those of you with the power to change things now will adopt new or amend existing policies to include these sharp insights. Other pitches will be refined with careful ruminations and further iterations. Each idea is a piece of a large puzzle that will help our societies be more prepared to respond to malicious foreign interference and ultimately become more resilient.

Students, we applaud you.

Piret Pernik, CCDCOE
Kathryn H. Floyd, William & Mary
Teresa Longo, William & Mary

PART I:
PATRICIPANTS AND PARTNERS

25+ TEAMS FROM 28 UNIVERSITIES
130+ STUDENTS FROM 16 COUNTRIES

- United States Air Force Academy
- Algebra University College
- Ashland University
- Berea College
- Bergische Universität Wuppertal
- Brescia University
- Bucknell University
- Carnegie Mellon University
- CEVROINSTITUT [vysoká škola]
- UCONN University of Connecticut
- JMU James Madison University
- ODTÜ METU
- Academia Navală Mircea cel Bătrân
- UNG University of North Georgia
- Old Dominion University
- University of Oxford
- Özyeğin University
- UPT Universitatea Politehnica Timişoara
- Sapienza Università di Roma
- University of St Andrews
- Texas A&M University
- Texas The University of Texas at Austin
- University of Toronto
- United States Military Academy West Point
- Universidad de Navarra
- University of Public Service Ludovika
- Karazin University V.N.Karazin University
- William & Mary Chartered 1693

PARTICIPATING UNIVERSITIES

Algebra University College (Croatia)
Arizona State University (USA)
Ashland University (USA)
Bergische Universität Wuppertal (Germany)
Brescia University (USA)
Carnegie Mellon University (USA)
CEVRO Institute (Czechia)
James Madison University (USA)
Leiden University (Netherlands)
Middle East Technical University (Turkey)
“Mircea cel Batran” Naval Academy of Constanta (Romania)
Old Dominion University (USA)
Ozyegin University (Turkey)
Polytechnic University of Timisoara (Romania)
Sciences Po-Reims (France)
Texas A&M University (USA)
United States Military Academy (USA)
Università di Roma La Sapienza (Italy)
University of Bucharest (Romania)
University of Connecticut (USA)
University of North Georgia (USA)
University of Oxford (UK)
University of St Andrews (Scotland, UK)
University of Texas at Austin (USA)
University of Toronto (Canada)
USAF Academy (USA)
V.N. Karazin Kharkiv National University (Ukraine)
William & Mary (USA)

JUDGES AND MENTORS

Mentors

Roger Yee
Managing Partner, outcome/one

Mateusz Buczek
Cryptographer/Cyber Security, Crypto SME

Guillermo Colell
Executive Director of Strategy & Roadmaps, Innovation & Capabilities Office, ManTech International

Dr. Katharine Jennings
Senior Science Manager, Nobils, Inc.

Jay Walker
Managing Partner, Defense Entrepreneurship Forum

Mike Descher
Founder & CEO, MediaGroup

Dr. Elizabeth Losh
Professor of English & American Studies, William & Mary

Robin El Kady
International Staff, NATO HQ

Commander Jacob P. Galbreath
Strategy Branch Lead, CCDCOE

Dobril Radoslavov
Defense Policy and Palnning Directorate, Bulgarian MoD

Michael Dick
Visiting Proessor and Co-Director, Puller Veterans Benefits Clinic, William & Mary Law

LTC Nathan Colvin
Public Policy Fellow and Lecturer, William & Mary

John Linantud
Professor and Coordinator of Political Science, University of Houston Downtown

Fabio Biondi
Deputy Branch Chief of Plans and Exercises, Italian MoD Cyber Command

Paul King
Editor/Engagement Officer, NATO

Alex Anvari
Advisor, Oracle

Keith J. Masback
Principle Consultant, Plum Run LLC

COL. Ben Miller (U.S Army Retired)
CWMD & CBRNE Senior Manager, Noblis

Charlie Foster
Director, W&M Office of Student Veteran Engagement

PART II:
AGENDA AND CASE STUDY

WMGIC x NATO Disinformation Challenge Event Schedule

3rd November 2023

8:00-8:20 a.m. EST

Opening Ceremony

Dr. Teresa Longo
Associate Provost for International Affairs, Executive Director of the Reves Center for International Studies, William & Mary

Reese O'Brien
Co-President, WMGIC

Dorothy Gao
Events Director, WMGIC

Sofia LoBue
Research Director, WMGIC

Shradha Dinesh
Disinfo Lab

Keynote Address - Stephen E. Hanson
Lettie Pate Evans Professor of Government, William & Mary

8:30-11:00 a.m. EST

Mentoring Session
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.

11:05 a.m. EST

Teams Submit Presentations
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.

11:20-12:40 p.m. EST

Presentations
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.

12:40-1:00 p.m. EST

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

1:15-2:00 p.m. EST

Closing Ceremony
Sophie Workinger
Co-President, WMGIC

Elizabeth Marcus
Events Director, WMGIC

Closing Remarks
Marie-Doha Besancenot
Assistant Secretary General for Public Diplomacy, NATO

Captain Kathleen Jabs
Special Assistant to the President for Military & Veteran Affairs, William & Mary

CASE DOCUMENT FOR UNDERGRADUATE TEAMS, MENTORS, AND JUDGES

OVERVIEW

The WMGIX x NATO HQ Countering Disinformation Challenge consists of six unique case topics. Each stream outlines a disinformation topic and challenge statement that you will seek to answer within the competition parameters and from 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. Remember, 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 disinformation. Presentations will be judged by criteria listed within the case document. One winning team will be chosen from each of the streams to give a three-minute presentation at the closing ceremony and recieve a cash prize. Winning teams are invited to produce a one-page infographic about their solutions. Additionally, competitors have the opportunity for their solutions to be published following the competition. Throughout the competition, all participants are encouraged to network with judges and mentors.

CASE DOCUMENT FOR UNDERGRADUATE TEAMS, MENTORS, AND JUDGES

RULES AND PARAMETERS

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

The cases 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 EST) to the deadline (11:00 am EST) to work on their project and create all deliverables.

CASE DOCUMENT FOR UNDERGRADUATE TEAMS, MENTORS, AND JUDGES

DELIVERABLES

Submit a five-slide maximum PowerPoint/PDF slide deck including a slide with a 150-word project summary. Please submit the presentation by 11:05 am EST.

Present a three-minute (maximum) PowerPoint presentation to the judges, including action item(s), outputs, potential NATO HQ implementation, and the 150-word project summary slide.

Participate in a three-minute Q&A session with the judging panel.

The winners 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. After the competition, winners are invited to produce a one-page infographic about their solutions that may be used in the post event book and by NATO.

WMGIC'S SUGGESTIONS ON HOW TO BEST UTILIZE MENTORING TIME

As part of the WMGIC x NATO HQ Countering Disinformation Challenge, you will meet with two mentors for 15 minutes each. These mentors are experts in the field of national security and disinformation and can help you gain context into the real world. Mentors are there to enhance your project, give you context into the real world, and utilize their expertise to help you. Being prepared for mentors and effectively utilizing their guidance and knowledge can help turn a project from great to exceptional.

CASE DOCUMENT FOR UNDERGRADUATE TEAMS, MENTORS, AND JUDGES

WMGIC'S SUGGESTIONS ON HOW TO BEST UTILIZE MENTORING TIME

Once you receive the event packet, please take a look at the names of your mentors. Their positions and biographies are all on our website, so take some time to look over this information so you know their areas of expertise and how they can best help you. You have a limited time with mentors, so you do not want to spend more time than necessary having the mentors giving you their background.

On the day of the competition, a few minutes before your mentor enters the room, communicate with your teammates to form a list of questions that you may have, things that you are worried about, or how mentors can use their expertise to help you. It can also be helpful to ask mentors about how they can use their expertise to help you. We recommend that you spend no more than five minutes summarizing your approach. You should spend the bulk of your time asking questions and getting input on specific areas of your project.

If you are stuck on how to kickstart the conversation, the WMGIC team has come up with a list of potential questions to ask mentors.

- After listening to our idea, are we on the right track?
- We have a few ideas, can you help us narrow down which one we should focus on?
- We are stuck on [x], can you help us brainstorm a solution?
- How can we best tell our story and articulate why our idea is the best?
- What are some holes in our project or things we have not considered?
- Are there any parts of our project that are unrealistic in the real world?

If you believe that your time is better spent talking amongst your teammates internally or working on your outputs, you can ask the mentor to listen in and have them interrupt when necessary. If you truly believe that having a mentor in the room is not of added value, you can kindly tell them that while you appreciate their time, they can head back to the main zoom room while you research, write, or plan amongst your team.

JUDGING CRITERIA

Feasibility & Effectiveness: (1-5)
Is it a potentially effective solution to address the problem? Does the plan follow the rules and regulations of the competition (i.e., budget, scope)? Does the project have performance metrics and evaluation incorporated into its plan?

Creativity: (1-5)
Do solutions show strategic thinking that utilizes 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: (1-5)
How can you keep the privacy of online, in particular social media, users while still analyzing 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? Does the project comply with existing privacy laws in NATO countries? How does the project protect the right to freedom of speech?

Sustainability: (1-5)
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 solution have the potential for future growth?

Fiscal Pragmatism: (1-5)
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?

INTRODUCTION TO DISINFORMATION

Disinformation is the “deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead.” Disinformation exacerbates nearly every domestic and global challenge, from election security to climate change. Its global spread can have profound consequences, including inflamed social conflict and unrest, distrust of the media and/or government, the spread of discredited science/medicine (e.g., the use of ivermectin to treat COVID-19), and the undermining of democratic elections.

NATO recognizes the urgency of countering disinformation, and the Alliance has taken substantial steps to do so over the last decade. In the 2018 Brussels Summit Declaration, the 2019 London Declaration, and the 2022 Strategic Concept, the Alliance has recognized the need to develop strategic responses to disinformation campaigns that seek to undermine international norms. The 2023 Vilnius Summit Communique strongly recognizes the need to counter disinformation. NATO has prioritized countering disinformation through a variety of means including proactive communications, “pre-bunking,” and debunking, such that the Alliance can inform civilians of misleading information before it proliferates online. However, the challenge of developing comprehensive and coordinated responses to disinformation persists for NATO.

The case documents below offer overviews of some of the most pressing issues implicated by disinformation. These documents are an introduction for teams to begin their research and solution development–not a comprehensive report on the subject matter.

DISINFORMATION STREAM OPTIONS

Clean Energy
Public Health
Sexism and Gender-Based Violence
Terrorism
Human Rights
Russia-Ukraine War
Artificial Intelligence (AI)
Climate Security

WMGIC AND NATO COLLABORATE FOR 4TH ANNUAL GLOBAL DISINFORMATION CHALLENGE

Lydia Urban, W&M News

William & Mary's Global Innovation Challenge (WMGIC) partners with NATO to host the WMGIC x NATO Countering Disinformation Challenge for the 4th consecutive year.

The event will be held virtually over Zoom on Friday, November 3, 2023, from 8am-2:00 pm EST. The competition's opening ceremony will be at 8am ET (1:00pm GMT) and broadcasted live on Zoom (registration is required).

"After last year's remarkable success, we're honored to partner with NATO once again for the WMGIC X NATO Countering Disinformation Challenge," says Dorothy Gao '24, WMGIC Events Director. "This year, we have updated our case document, incorporating the most current disinformation concerns, and introduced an entirely new Human Rights stream. We can't wait to see what the brightest young minds around the world can come up with to address these pressing disinformation issues!"

At the start of the challenge, student teams will be provided with an in-depth case study pertaining to one of eight streams. Collaborating with their mentors, students will formulate a strategic blueprint for NATO's implementation over the coming 12 months, incorporating essential contextual insights, including specifics on the strategies employed by major nations and proxy organizations.

Panels of expert judges will evaluate the proposals and select eight winning teams, one from each stream. The winners will be announced at the conclusion of the Challenge in a live Zoom event/webinar from 1:15pm to 2:00pm ET (6:15pm-7:00pm GMT). There is a cash prize for the winner of each stream.

This Challenge is open to undergraduate students of all experiences and majors, in universities nationwide and internationally from NATO Member Nations. The entire event is conducted in English. Each team will comprise three to five students.

Innovation Through Collaboration

The Global Innovation Challenge (WMGIC) is the premier intercollegiate international and sustainable development case competition aimed at encouraging interdisciplinary collaboration to create innovative solutions for current global issues.

Founded in 2017 by William & Mary students, WMGIC offers an avenue for undergraduate students globally to engage in collaborative discussions with peers, faculty, and experience experts. It serves as a platform for the exchange of innovative solutions and ideas aimed at improving the future.

WMGIC Partnership with Whole of Government Center of Excellence and the Reves Center for International Studies.

WMGIC is being advised by the Whole of Government Center of Excellence (WGC) and the Reves Center for International Studies for this year's event. WGC and Reves aim to inspire crucial discussions and relationships between students and security priorities around the world.

Students interested in participating in the WMGIC x NATO Countering Disinformation Challenge may learn more about the requirements and submit their applications online.

The deadline to register has been extended to October 30th, 2023.
Experts interested in serving as mentors for this or future WMGIC Challenges may contact wgc@wm.edu.

PART III:
WINNING PITCHES

ALPHA STREAM:
TEAM NAME: GLOBAL DISINFORMATION LAB

AUTHOR NAMES: Jewells Escamilla, Riley Galligher, Samantha Tanner, Britany Tran, Isabella Sherwood

AFFILIATIONS: University of Texas at Austin

SUMMARY: Deepfake videos of prominent world leaders are often used to spread disinformation and sow discord among citizens of NATO states. This project will verify the authenticity of social media content about NATO government figures by creating a forensic watermark given to member states to embed in government-generated content, and tracking the metadata of such content. Through partnerships with social media platforms, existing automated systems will screen posts containing content of NATO member-state government figures to ensure it contains the NATO watermark and accurate metadata. Verified content will be labeled as "verified," while content failing this verification will be "flagged.” Automated decisions will be reviewed by a human task force to enhance accuracy, enabling social media users to easily distinguish manipulated content from authentic posts. This project aims to combat the spread of disinformation by deepfakes and enhance trust among citizens of NATO states.

BRAVO STREAM:
TEAM NAME: MAPSTONE’S MONSTERS

AUTHOR NAMES: Joseph Atkinson, Connor Burleigh, Ava Pourfallah

AFFILIATIONS: University of St Andrews

SUMMARY: The livestream approach allows for concerns/disinformation in public health to be addressed in an engaging and formative manner. The panels also act as a verification process through which different actors from different backgrounds validate the information provided. The panel then creates content which can be dispersed as engaging content through various social media platforms. The social media platforms for the events would also have question submission portals allowing questions for the panel to discuss. These questions will be filtered but also allow direct engagement with the publics concerns relating to disinformation and public health. The submitted questions can also be used to identify developing trends in disinformation and these can be incorporated into the streams discussion bases. The virtual basis of the panel also allows for engagement and countering disinformation relating to public health when due to a public health crisis in person engagement may be impossible.

CHARLIE STREAM:

TEAM NAME: NATO AMBASSADORS OF PEACE

AUTHOR NAMES: Denis Beber, Mara Bulzan, Eduard Lupșescu

AFFILIATIONS: Sciences Po-Reims, Polytechnic University of Timișoara, University of Bucharest

SUMMARY: Inspired by Romanian's underreporting of sexism and gender-based violence by high-profile populist politicians, our AI-based approach tackles disinformation for two main sources of spreading false information: online mass media and social media. This fact-checking AI will employ data integration to process various sources of what we consider reliable statistics coupled with Natural Language Processing to cross-reference with data transmitted by politicians in mass media and shared by users of social media. It will especially consider domestic abuse, human trafficking, reports of sexual and gender-based violence used for war propaganda and sexual harassment. The AI, in the form of either a browser extension or an app, would flag online information perceived as unreliable and would label it with the data considered highly reliable instead. It would be mandatory for mass media and highly promoted for social media users. Therefore, our approach mitigates politicians' manipulation of official data and corrects erroneous information.

DELTA STREAM:

TEAM NAME: SOLO 4

AUTHOR NAMES: George Barton, Kasper Hong

AFFILIATIONS: William & Mary, Carnegie Mellon University

SUMMARY: StratCom can powerfully challenge the Taliban narrative of disinformation by creating a global media outlet led by a united diaspora of Afghan journalists. Through partnering displaced Afghan journalists with citizen reporters still inside the country, this media initiative engages the Taliban on the cognitive dimension. Following 2021, hundreds of Afghan journalists fled to Pakistan and Iran, but now face deportation. While US efforts to grant asylum are overwhelmed by demand while being stalled by Pakistani authorities, NATO countries can provide refugee status for Afghan journalists and connect them to existing activist networks. Digital technology has made it easier for professional journalists to connect with anonymous sources, but lapses in security have exposed and harmed citizen journalists. To mitigate these issues, we emphasize using secure messaging apps with encryption paired with online anonymizing tools. Additionally, formulating emergency plans, fostering support networks, and providing medical training can increase safety and effectiveness.

ECHO STREAM:

TEAM NAME: DISINFORMATION DESTROYERS

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

AFFILIATIONS: William & Mary

SUMMARY:
Disinformation surrounding human rights threatens the reputation of NATO member-states, actively works to impede NATO missions, and challenges NATO values and global leadership. NATO must respond to these instances of disinformation and censorship with engaging counter-messaging and educational resources. We propose a “NATO News Room” that would feature short-form content across social media platforms like TikTok and Instagram. These videos would address specific human rights-related issues determined by our priority risk assessment framework and provide known facts as well as credible resources for more information. The goal of our solution is to create impactful and engaging content to combat human rights abuses that are exacerbated by disinformation. The News Room will feature content in multiple languages and will utilize artificial intelligence to compete with the virality of disinformation campaigns. Our pushes the limits of current NATO norms, but this kind of creativity is necessary to adequately address the disinformation problem.

FOXTROT STREAM:

TEAM NAME: MADISONIAN DEFENSE

AUTHOR NAMES: Nicole Capaldo, Justin Frye, Omer Mutlu, Isabella Santos

AFFILIATIONS: James Madison University

SUMMARY: The NATO alliance should partner with an outside organization to create a docuseries outlining the history of Russian propaganda and how it has developed over time, culminating in their recent efforts surrounding the invasion of Ukraine. The series will be a five episode format, with each being forty-five minutes in length. An entertainment format will ensure that NATO reaches an audience that a traditional platform may neglect. A third party should oversee the production of the project to offset costs that the alliance must bear and add credibility to the series. NATO can maintain a level of control over the narrative of the show by offering access to high level officials for interviews. Lastly, the docuseries creates a sustainable marketing campaign free of additional cost. By tracking metrics, NATO can turn clips from the series into social media posts highlighting arguments and topics that resonated the most with viewers.

PART IV:
OTHER PITCHES

ALPHA STREAM: Artificial Intelligence

TEAM NAME: Old Dominion University

AUTHOR NAMES: Jada Cumberland, Elijiah Gartrell, Brandon Zakaras

AFFILIATIONS: Old Dominion University

SUMMARY: We propose that NATO starts a council for the creation of a framework for policies regarding deepfaking indicators when an image or video is uploaded to a platform. In year one, companies across the world and from different industries would be invited to collaborate to build a set of standards to handle the identification of deepfakes similar to the NIST Cybersecurity Framework. This could include review procedures and deepfake indicators, similar to those present on platforms like Instagram and X (formerly known as Twitter). Companies would be likely to use it as handling AI has become an issue that can affect their security now and in the future. Additionally, those involved in its creation would be naturally likely to adhere to the created policies. Although a framework cannot be fully created in a year, this solution would be ever-changing as a reflection of the nature of technology.

TEAM NAME: The Old Team

AUTHOR NAMES: Vlad Catalin Costin, Timofte Mihai-Danut, Gheorghe Andrei Dorian

AFFILIATIONS: “Mircea cel Batran” Navala Academy of Constanta

SUMMARY: A website designed to analyze and detect manipulated content serves a crucial role in the public's digital landscape. Recent events have shaped the way information is presented online. In an era rife with deepfakes, misinformation, and image manipulation, such a platform offers several compelling advantages. Firstly, it empowers individuals to be discerning consumers of media and teach them how to discern an information from propaganda. Users can verify the authenticity of images, videos, and audio, enabling them to make informed decisions and avoid falling victim to deception.

Secondly, it aids professionals, including journalists and fact-checkers, in their efforts to maintain the integrity of news and information. By providing access to a medium in which like-minded individuals can gather and offer knowledge through an open source platform, the website supports accurate reporting and upholds the credibility of social-media.

TEAM NAME: Mighty Falcons

AUTHOR NAMES: Anjulina Abdon, Allison Langenburg, Arianna Pontoni, Sonia Tegang, Ryan Torres

AFFILIATIONS: United States Air Force Academy

SUMMARY: To effectively confront the most influential actors threatening freedom of information in the digital age, NATO should establish a collaborative task force capable of generating a deepfake detection database. This task force's primary objective is to enhance the collective ability to counter disinformation and maintain the integrity of information within the framework of the liberal world order. As part of its assignment, this NATO task force will focus on collecting and disseminating information related to influential actors actively participating in the digital age of disinformation. Additionally, it will prioritize investments in cutting-edge algorithms for detecting evolving deepfake technologies. Within this framework, member countries can elicit aid from global experts who are crucial to the task force, addressing the challenges of deep fakes and disinformation within their respective states. In pursuing this outcome, NATO aspires to set international standards encompassing transparency, institutional credibility, information sharing, and global cooperation.

TEAM NAME: Muove

AUTHOR NAMES: Nanxi Lu, Melanie Quach, Dong Syuan Tan, Ziang Zhou

AFFILIATIONS: University of Connecticut

SUMMARY: The proposed Collaborative Programme of Work within NATO, dedicated to detecting deepfakes, will align alongside partnering with specialists like Truepic, will develop algorithms to evaluate the likelihood of AI-generated content on social media. Data analysis will involve three key metrics: AI probability, weighted topic ranking and report rates. Thresholds will trigger a deeper investigation by a multidisciplinary expert group. Confirmed deepfakes will be posted on the official forum, as well as the activities of the CPoW. Parallelly, an advertising campaign will educate the public on deepfake recognition, leveraging the Mere Exposure Effect through repeated exposure on various platforms, thus enhancing societal resilience against deepfake deceptions.

TEAM NAME: Solo 1

AUTHOR NAMES: Vanessa Broadrup, Dannise Brown, Matteo Vastante

AFFILIATIONS: William & Mary, "La Sapienza" Università of Rome, James Madison University

SUMMARY: Our proposal entails an educational outreach campaign targeted towards policymakers across NATO allied countries. With evolving AI and deepfake technology, it is paramount that policymakers understand existing relevant laws and regulations. We seek to use DIANA as a framework to cultivate policy ideas and research using its existing connections. Using DIANA will enable low upfront costs in the first 12 months of this program. The program will make use of lawyers and legal experts from private businesses and in the field of AI to effectively legislate. It will make it easier for companies to conduct business via the sharing of AI technologies and to conduct business in NATO member countries while navigating the emerging challenges AI poses.

TEAM NAME: YATA Hungary

AUTHOR NAMES: Gréta Kiss, Ignác Murányi, Dóra Paszternák, Málna Szonja Vámos

AFFILIATIONS: University of Public Service Ludovika

SUMMARY: We would like to create a common information sharing environment (platform) where NATO allows its members to share any gathered deep fake created open-source information. This cloud-based solution facilitates data sharing with standard data analysis tools that enable collaborative intelligence analysis. The platform enables national intelligence to the fusion and integration of various data sources, including open-source data, classified information, and signals intelligence, to provide a comprehensive view of threats. Selected Centers of Excellence (COEs) would serve as the hubs of gathered data. COEs can define and promote standards and practices for data sharing and establish guidelines for data classification, access control, compliance with relevant regulations. COEs can work on building and maintaining corporations with international intelligence partners, ensuring the platform aligns with collaborative efforts on Alliance scale. For the first year, the goal is to develop a technical infrastructure and establish a standard structure of information sharing practice, which enables the gathered information to be analyzed collectively by humans and machines.

TEAM NAME: Roger’s Rangers

AUTHOR NAMES: Ferdinand Kříž, Charlotte Maria Loštická, Ondřej Olšanský, Natálie Skokanová

AFFILIATIONS: CEVRO Institute, Charles University, Czech Defence University

SUMMARY: Our main concern in regard to information warfare is that NATO is inherently reactive in its approach to countering adversary psyops and influence operations. We propose implementing reflexive control approaches into standing NATO Influence and psyops strategic documents (i.e. AJP 3.10.1, AJP 3.10, AJP 10.1). This approach leverages already existing bodies and units tasked with hybrid/information warfare. Concerned units are already established within NATO member states armed forces, have set and exercised SOPs and defined ROEs. Leveraging these structures would result in reduced cost of implementation while adhering to the national and supranational legislation. We view this approach not as a singular measure to countering Russian influence operation, but as a toolbox complementing wider range of Operational measures, both defensive and offensive (debunking, pre-bunking, etc.). Amending standing strategic, operational and tactical ROEs and SOPs with reflexive control measures would create holistic toolbox with global application surpassing current Russian problem.

PART IV:
OTHER PITCHES

BRAVO STREAM: Public Health

TEAM NAME: Solo 3

AUTHOR NAMES: Lovro Fabijanić, Ian Harman, Seher Kaur Sethi

AFFILIATIONS: William & Mary, Algebra University College

SUMMARY: RETINA (Real-engaging-transformative-information-neutral-asset) is an application used as an extension to social media that is made to detect misinformation and give the user more credible data sources to look into the subject. It uses datasets from open source to identify potentially risky posts and accounts and then presents the user with a simple infographic that breaks down the analysis algorithm and highlights what makes the post credibility questionable. It also offers referrals to trusted information sources backed by numbers, also highlighting the numbers given through different referral sources. It's NGO funded, with NATO's initial investment made to support development and endorsement as a functional tool.

TEAM NAME: University of North Georgia Nighthawks

AUTHOR NAMES: Marc Bilia, Zachary Furbush, Dylan Gearin, Nathanael Hines, Rubi Islas

AFFILIATIONS: University of North Georgia

SUMMARY: The NATO Counter Information Initiative requires the cooperation of Member States and media companies. The initiative has three main components: the Accurate Information License (AIL), the Integrity Board (IB) and Counter Information Campaigns (CIC). AIL will be available for all media companies to apply. It acts as a certification for media outlets that the IB determines are less likely to create disinformation and spread misinformation. The IB consists of specialized experts and health ministers. For the sake of Public Health, these experts will have a background in medicine or biology. CIC will create targeted responses to disinformation by spreading confirmed and accurate information. Media and advertising companies will benefit from this through incentives such as priority in NATO contracts, subsidies, state sponsored tax benefits, public prestige, and other incentives. The goal of this initiative is to erase the monetary incentive of spreading disinformation and promote the spread of accurate information.

TEAM NAME: Bearcats International

AUTHOR NAMES: Henry Chingaipe, Talon Hutto, Elkana Mongare, Juan Tavera

AFFILIATIONS: Brescia University

SUMMARY: Our solution involves pre-bunking the spread of disinformation amongst the public health sectors through artificial intelligence and partnering with Non-Governmental Organizations while using the Public Diplomacy Division. This amplifies what NATO has previously done to combat the COVID-19 disinformation trends from countries, such as Russia and China. This solution can be used in crisis scenarios, aka preventing the spread of infectious diseases. This reinforcement will broaden to all countries in the alliance. The NGO used will be the Association for the Advancement of Artificial Intelligence (AAAI). AAAI will provide production knowledge for our AI method as well as funding for implementation, mixed with the PDD's portion of the NATO Civil Budget. This project will cost roughly $200k USD, which is about .05% of the NATO Civil Budget. This cost includes both pre-bunking and a fact-checker element. Using artificial intelligence as a fact-checker will put notice to disinformation trends before spreading.

PART IV: OTHER PITCHES

CHARLIE STREAM: Sexism & Gender-Based Violence

TEAM NAME: UNAV – Security & Defence

AUTHOR NAMES: Sara Hernandez Calabrés, Lulu Victoria Gonzalez, Paula las Heras Martinicorena, Nathalia Maria Lozano Murphy, Ivanna Maria Salome Simon

AFFILIATIONS: Universidad de Navarra

SUMMARY: NGS (NATO GEN-SAFESHIELD or NATO Gender Equality and Security Shield) is a NATO-led initiative to tackle gender disinformation through: First, develop media literacy programs to educate the public on how to critically assess news sources, identify disinformation, and recognize gender biases. Also, media campaigns through contemporary social media outlets which allow for the connectivity of the issue to the popular public, for example, the use of tiktok. Second, the creation of a digital platform that provides legal services and support across the alliance without a language barrier. The platform is made up of regional teams that focus on specific legal frameworks and provide assistance to women that have suffered from disinformation effects or gender based violence. Lastly, develop an annual report, which evaluates the different cases and responses implemented, and implement a preventive approach. All of this, protecting the victims privacy and partnering with NGOs, which are experts on the topic.

TEAM NAME: The Transfers

AUTHOR NAMES: Can Bostancı, Riley Coler, Furkan Makinacı, Eylül Seneger

AFFILIATIONS: Middle East Technical University, Bilkent University, Leiden University

SUMMARY: We will commence by establishing a network of female journalists to raise awareness within civil society. Harnessing this awareness, we will initiate government-subsidized projects to make AI and MLM tools more gender-neutral for the detection of gender-based violence. Engagement with the government is vital, particularly in regions such as Turkey, where media is government-controlled. To achieve this, we will leverage the civil networks built by female journalists and numerous gender-focused NGOs. Collaborating with the government is crucial. For long-term sustainability, we plan to tap into the government's media influence to create a pioneering beta project in Turkey. The ultimate goal is to transform this initiative into an international project within NATO and neighboring countries. By forging partnerships with civil society and government stakeholders, our objective is to foster a safer, more inclusive environment for female journalists, setting an example for broader global change.

TEAM NAME: Diplomaslay

AUTHOR NAMES: Carlee Blankenship, Jessica Case, Orla Fennel

AFFILIATIONS: University of North Georgia

SUMMARY: We seek to establish a multistakeholder task force to promote and increase digital literacy. Our digital literacy initiatives will be interactive and engaging, and resemble a former interactive-awareness technology called Admongo. When looking at past NATO responses to disinformation we found infographic competition that NATO did in partnership with Facebook. With this format in mind, we think that this competition can be redesigned to teach about common disinformation target actions. We also seek to provide incentives including giving companies trust marks and awarding the winners of the competition. In regards to AI, we want to provide anonymous surveys to integrate the human aspect and in turn, create better AI detection features. Digital literacy campaigns are costly, estimated at 6-11 billion USD. We plan to seek funding from the NATO Diana Fund, U.S. Department of Education, Office of Career, Technical, and Adult Education, European Education Area, and private sector.

PART IV: OTHER PITCHES

DELTA STREAM: Terrorism/Taliban

TEAM NAME: Ashland University AHS Team 2

AUTHOR NAMES: Mekenzie Flora, Cole Jenkins, Tyler Suppes

AFFILIATIONS: Ashland University

SUMMARY: In this project, the end goal is to stop harmful statements from being spread by terrorist organizations. In that spirit we also are wanting to increase education on how to be smart users on social media sites to then stop disinformation from spreading severely. We would work with NATO in order to create a multi-national commission whose purpose would be to work on the algorithms of the social media sites, dealing with artificial intelligence (AI) systems and simultaneously informing the human users of these same sites. These new creations would be a baseline for these sites, and it would allow for a safer cyberspace. We would create an extension that would help with fact checking and then would also be up for review to AI and the commission. Speed and efficiency are a key concern, so AI will be used to screen posts immediately upon their upload; human moderation of flagged posts will ensure measures are within the bounds of international law.

TEAM NAME: Ashland University AHS Team 1

AUTHOR NAMES: Nora Bacon, John Cartigione, David Maloney, Robert Mouledoux, Matt Savage

AFFILIATIONS: Ashland University

SUMMARY: Regarding our plan to combat misinformation from the Taliban on social media, we are approaching the issue as a two pronged approach. The first prong will involve a satellite radio station with exiled Afghan broadcasters that will be available to Afghani listeners that reports information from the outside world; including news of other Arab nations, current world events, cultural Islamic news and content, and reports of Taliban activity from an objective, outside perspective. The second prong will involve a third party fact-checker technology, set up in collaboration with X (formerly Twitter) that uses fact-checkers specifically targeting the Taliban's accounts to censor misinformation and reduce the volume of information spread by the Taliban. Both sections will be run out of a non-profit research organization that is collaboratively set up between NATO and the OSCE, both contributing funds and workers in order to share the burden of combating misinformation in both regards.

TEAM NAME: Truth Social

AUTHOR NAMES: Leonie Henkel, Jakkob Kaiser, Lea-Marie Kurp, Joshua Siepe

AFFILIATIONS: Bergische Universität Wuppertal, DHBW Mannheim

SUMMARY: NATO as a platform where the most relevant and latest misinformation is summarized/consolidated. Such initiatives already exist at national or regional levels but not through institutions of such international reach and legitimacy. NATO should host a competition to reward discovery and debunking of disinformation. Only contributions by individuals are accepted. The most valuable contributors would be rewarded by NATO to foster a competitive environment. Findings/contents are intended to be primarily published in social networks where we suspect a great share of our target audience: Predominantly male, young adults and adolescents from unsteady backgrounds prone to influence by populist and radical movements - such as the Taliban. It is important to keep in mind that counteractions of terroristic groups such as the Taliban should anticipated. An upscaled version of the project should lead to a collection of relevant information and strategies as a database for future situations.

PART IV: OTHER PITCHES

ECHO STREAM: Human Rights

TEAM NAME: Team Texas

AUTHOR NAMES: Hugh Coleman, Alan Crabb, Somkar Dey

AFFILIATIONS: William & Mary

SUMMARY: Religious violence threatens human rights. Cartoons can counter violence by satirizing pointless hatred. Political cartoons in mainstream foreign newspapers could build on NATO's media campaigns to reach wide, diverse audiences. Cartoons would highlight the absurdities of inter-religious conflicts, like Hindus and Muslims attacking each other's mosques and temples. This could encourage questioning among extremists. Cartoons are nonviolent communication tools that align with NATO values. While not solving fundamental theological divisions, cartoons can reduce hostility and soften attitudes. Humor and satire deflate dogmatic rage. Cartoons won't eliminate militancy but may open minds. Gradually undermining rigid mentalities, cartoons can calm religious tensions. A long-term communications strategy using incisive cartoons in popular media could relieve religious divides. Promoting religious pluralism and respect, cartoons demonstrate shared humanity despite different faiths. Using existing NATO media channels, cartoons can promote tolerance and undermine extremism.

TEAM NAME: Calvin & Hobbes

AUTHOR NAMES: Simon Fox, Ding–Yuan Hsin, Maggie Jacobs-Weeks, Phillip Matijevic

AFFILIATIONS: William & Mary

SUMMARY: We have created a two-pronged approach to countering human rights disinformation. Our short-term approach is modifying social media platform practices verifying community fact check, and tweak social media algorithms. On social media, we promote non-monetary verification (i.e. must be checked with an ID and not paid for.) We would also encourage the use of open-source fact-checking for political and current event-related posts and stories (similar to open notes on Twitter with some important modifications), and lastly, we would suggest that social media platforms revise their algorithms on political news feeds, meaning that a user would not just be touted stories strictly conforming to their social media views, but presented with a variety of views instead. The long-term approach to halting the spread of disinformation would be a curriculum created by NATO and presented to member states to aid with their media literacy education. Teaching media literacy as young as elementary school is crucial to forming a generation that can recognize disinformation. Such a curriculum would include checking the credibility of a source, being extremely wary of news posted on social media, and questioning the biases of journalists and authors of any source.

PART IV: OTHER PITCHES

FOXTROT STREAM: Russia-Ukraine War

TEAM NAME: Sociofamily

AUTHOR NAMES: Kseniia Kikot, Ihor Lameko, Bondarenko Oleksandr, Anastasiia Soshenko, Ruslan Zaporozhchenko

AFFILIATIONS: V.N. Karazin Kharkiv National University

SUMMARY: The idea behind our project is that education is the most valuable resource in the modern world. In the context of hybrid warfare, which has all the hallmarks of cognitive warfare, it is possible to fight disinformation only by developing one's own knowledge, critical thinking, media literacy and practical skills to recognize and debunk disinformation. We propose to emphasize informal education that integrates with digital technologies. This education is free, simple and aims to train people to identify, distinguish and debunk fakes and misinformation. It could be a website or a mobile application that would create an online course with theory, videos on exposing disinformation, an interactive simulator, and practical exercises. An example of the implementation of such a project could be the Ukrainian digital platform Diia, which is already used by more than 18 million Ukrainians. The development of such a course can take several months.

TEAM NAME: USMA Black Knights

AUTHOR NAMES: Alexis Bradstreet, Ryan Henry, Maxx Simeon, Peter Toth

AFFILIATIONS: United States Military Academy

SUMMARY: More than one information war exists in the Russia-Ukraine conflict. Although NATO has been successful in building resilience to Russian disinformation within the Western audience, Russian narratives succeed in resonating among different groups—particularly the Global South. NATO must focus on counter-disinformation efforts with this audience as it threatens NATO's legitimacy around the world. We propose three main lines of effort in the Global South. First, utilizing regional journalism coalitions will promote the truth from trusted organizations in these regions. Second, developing inoculation-based media literacy interventions will address a gap in availability to non-Western populations. Finally, working with supply chains such as Meta will ensure that these platforms are also protecting a larger breadth of cultures.

Each of these lines of effort focus on preexisting solutions, which gives us high confidence in their success. Furthermore, they are likely to sustain in the future given their low maintenance requirements after initial investment.

TEAM NAME: Gig'em Bytes

AUTHOR NAMES: Geoffrey Bosenbark, Robert O'Reilly III, Lena Kazi, Oscar Leon

AFFILIATIONS: Texas A&M University

SUMMARY: Implementing the Counter-disinformation & Legitimate Evidence Alert Resource (CLEAR) is feasible and effective. Using Open-source Intelligence (OSINT) to gather and verify this information prevents intruding on privacy online in accordance with existing laws in NATO member-states. This approach is highly sustainable and can be implemented within a 12 month period.

TEAM NAME: Kasakela Chimpanzee Community

AUTHOR NAMES: Jack Keating, Spencer Krivo, Pooja Muthuraj

AFFILIATIONS: William & Mary

SUMMARY: We propose countering Russian disinformation by leveraging neural network machine learning and automated response algorithms for rapid identification and deterrence. This will involve, first, creating a neural network trained to detect social media posts containing Russian misinformation. Once identified, the network will direct a NATO-run botnet to flag the post and inform the public via social media platforms of its unreliability. By leveraging emerging technologies, this proposal will effectively counter the otherwise unmanageable volume of Russian misinformation. Additionally, it is both cheap and sustainable, requiring little in overhead costs and even less in maintenance, and increasing efficiency and effectiveness as the neural network is exposed to more misinformation and adapts to new Russian tactics. This policy will be simultaneously effective and cognizant of privacy and free speech rights—avoiding restricting social media users from communicating freely on the platforms, and operated transparently by NATO with expertly vetted information.