Published by CCDCOE

WMGIC x NATO Countering Disinformation Challenge 2022

D. Gao, G. Hage, K. Pelletier, P. Pernik, K. Rachamallu, T. Sterns, S. Workinger (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

WMGIC
GLOBAL INNOVATION CHALLENGE

WILLIAM & MARY
CHARTERED 1693

Published by CCDCOE

WMGIC x NATO Countering Disinformation Challenge 2022

D. Gao, G. Hage, K. Pelletier, P. Pernik,
K. Rachamallu, T. Sterns, S. Workinger (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

WMGIC
GLOBAL INNOVATION CHALLENGE

WILLIAM & MARY
CHARTERED 1693

WMGIC x NATO ACT Cybersecurity Challenge 2022

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

Copyright and Reprint Permissions

WMGIC x NATO ACT Cybersecurity Challenge 2022
Dorothy Gao, George Hage, Katie Pelletier, Piret Pernik, Kiran Rachamallu, Terra Sterns, Sophie Workinger (Eds.)
2023 © NATO CCDCOE Publications

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

LEGAL NOTICE: This publication contains the opinions of the respective authors only. They do not necessarily reflect the policy or the opinion of NATO CCDCOE, NATO, or any agency or any government. NATO CCDCOE may not be held responsible for any loss or harm arising from the use of information contained in this book and is not responsible for the content of the external sources, including external websites referenced in this publication.

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 decision-makers 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. 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.

TABLE OF CONTENTS

LETTER FROM THE EDITORS

The NATO Alliance and Partner Nations face many threats, many of which are invisible to the eye. Disinformation poses critical security risks in a manner of spheres and can easily affect entire nations. 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 Headquarters joined William & Mary's Global Innovation Challenge (WMGIC) and Whole of Government Center of Excellence (WGC) to task undergraduate students from across the Alliance and Partner Nations to tackle the problem of disinformation in seven unique topics.

The global record-breaking competition engages over 100 teams from over 50 universities to reach a total of over 400 competitors. On October 21, 2022, teams developed solutions to disinformation in the realms of Artificial Intelligence, Public Health, Gender-Based Violence, Clean Energy, Climate Security, Russia-Ukraine war, and Terrorism. Within seven hours, teams consulted expert mentors from around the world. Each team was then 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.

Nine teams were selected as the winners of their streams owing to their unique and tangible recommendations. As teams gave practical and sound advice to NATO HQ, the pitches of all undergraduate teams are contained within this publication. Their innovative ideas are 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 attribute it to the team who developed these solutions. After all, our participants are well equipped to become the next generation of world leaders.

We would also like to thank our chief supporters, the W&M DisinfoLab, the Whole of Government Center of Excellence, the Reves Center for International Studies, W&M VET, and the W&M Law School.

Dorothy Gao
George Hage
Katie Pelletier
Piret Pernik
Kiran Rachamallu
Terra Sterns
Sophie Workinger

FOREWORD

Preempting and countering disinformation is possible, but it does require proactive, well-coordinated action by the whole of society.

We all know that in our information space foreign state (primarily Russia, but also China) and nonstate hostile actors seek to influence and manipulate our publics' perceptions, attitudes and behaviours in support of their geopolitical aims. They strive to shake the confidence of our citizens in institutions and governments, to split societies and create confusion. This is a national security threat and various parts of society–governments, civil society, media, industry–have a responsibility to respond.

Addressing the dangers of disinformation was the focus of this edition of the William & Mary Global Information Challenge (WMGIC). This perilous challenge requires all hands on deck, especially the creative and passionate minds of youth. In reading this book, you will come across ingenious and creative ideas put forward by WMGIC students. These ideas and presentations were the result of just hours of work–I can't imagine the great impact of these great minds with more time.

And that is my challenge to the youth participants, but also young people in general. We are at a critical juncture in our collective history–Russia's attack on Ukraine is the first massive war in Euroatlantic area since World War II. Spreading disinformation is part of Russia's war doctrine. We cannot underestimate this threat to our security. Educate yourselves, your peers and friends, as well as your family. Prebunk and speak out against disinformation and help make your own and collectively all our societies safer and more resilient.

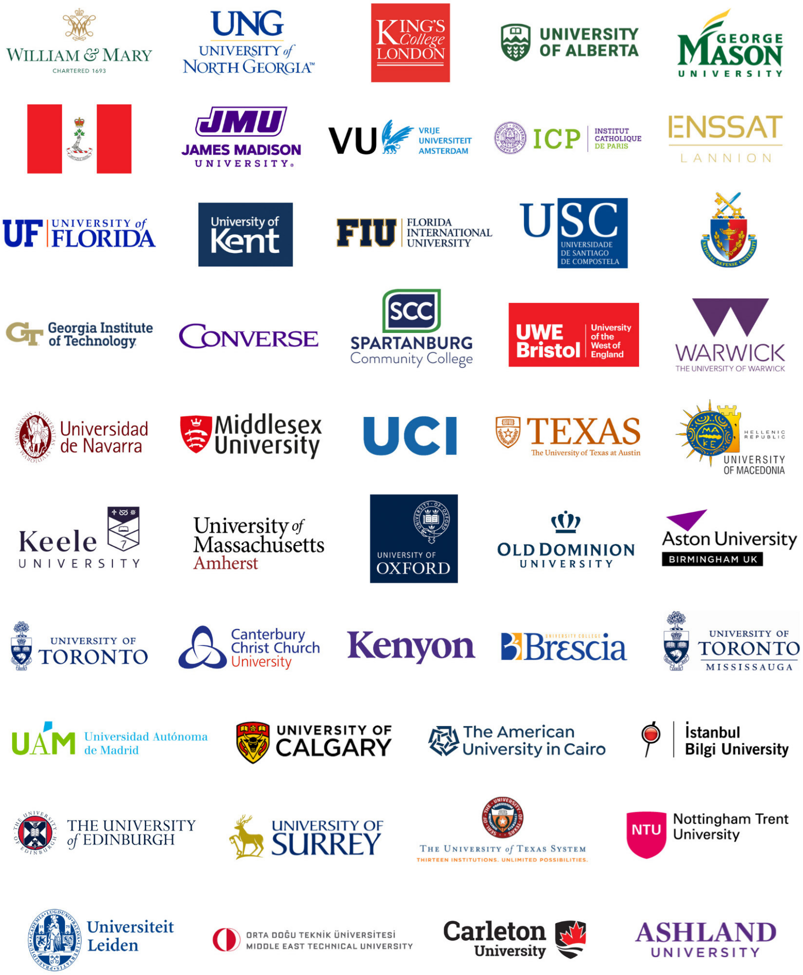
On a personal note, I hope all the participants try an internship or job with NATO in the future. We need your bright minds–continue to inspire us with your passion and ideas.

Baiba Braže
Assistant Secretary General for Public Diplomacy
NATO
30 June 2023

PART I:
Participants and Partners

Participants and Partners

63 TEAMS FROM 47 UNIVERSITIES


WILLIAM & MARY
CHARTERED 1693
UNG
UNIVERSITY of NORTH GEORGIA
KING'S College LONDON
UNIVERSITY OF ALBERTA
GEORGE MASON UNIVERSITY
JMU
JAMES MADISON UNIVERSITY
VU
VRIJE UNIVERSITEIT AMSTERDAM
ICP
INSTITUT CATHOLIQUE DE PARIS
ENSSAT
LANNION
UF UNIVERSITY of FLORIDA
University of Kent
FIU
FLORIDA INTERNATIONAL UNIVERSITY
USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
NATIONAL DEFENSE UNIVERSITY
Georgia Institute of Technology
CONVERSE
SCC
SPARTANBURG Community College
UWE Bristol
University of the West of England
WARWICK
THE UNIVERSITY OF WARWICK
Universidad de Navarra
Middlesex University
UCI
TEXAS
The University of Texas at Austin
HELLENIC REPUBLIC
UNIVERSITY OF MACEDONIA
Keele UNIVERSITY
University of Massachusetts Amherst
UNIVERSITY OF OXFORD
OLD DOMINION UNIVERSITY
Aston University
BIRMINGHAM UK
UNIVERSITY OF TORONTO
Canterbury Christ Church University
Kenyon
Brescia
UNIVERSITY OF TORONTO
MISSISSAUGA
UAM
Universidad Autónoma de Madrid
UNIVERSITY OF CALGARY
The American University in Cairo
İstanbul Bilgi University
THE UNIVERSITY of EDINBURGH
UNIVERSITY OF SURREY
The University of Texas System
THIRTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.
NTU
Nottingham Trent University
Universiteit Leiden
ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY
Carleton University
ASHLAND UNIVERSITY

PARTICIPATING UNIVERSITIES

The American University in Cairo (Egypt)
Ashland University (United States)
Aston University (United Kingdom)
Brescia University (United States)
Canterbury Christ Church University (United Kingdom)
Carleton University (United States)
Carol I National Defense University (Romania)
Converse University (United States)
CSD UNAV (Spain, Honduras, Colombia)
ENSSAT Lannion (France)
Florida International University (United States)
George Mason University (United States)
Georgia Institute of Technology (United States)
Institut Catholique de Paris (France)
Istanbul Bilgi University (Turkey)
James Madison University (United States)
Keele University (United Kingdom)
Kenyon College (United States)
King's College London (United Kingdom)
Leiden University (Netherlands)
Middle East Technical University (Turkey)
Middlesex University (United Kingdom)
Nottingham Trent University (United Kingdom)
Old Dominion University (United States)
Royal Military College of Canada (Canada)
Spartanburg Community College (United States)
Universidad Autónoma de Madrid (Spain)
Universidad de Santiago de Compostela (Spain)
University of Calgary (Canada)
University of California, Irvine (United States)
University of Edinburgh (United Kingdom)
University of Florida (United States)
University of Kent (United Kingdom)
University of Macedonia (Greece)
University of Massachusetts Amherst (United States)
University of Navarra (Spain)
University of North Georgia (United States)
University of Oxford (United Kingdom)
University of Surrey (United Kingdom)
University of Texas System (United States)
University of Texas at Austin (United States)
University of Toronto (Canada)
University of Toronto Mississauga (Canada)
UWE Bristol (United Kingdom)
Vrije Universiteit Amsterdam (Netherlands and Germany)
Warwick (United Kingdom)
William & Mary (United States)

JUDGES AND MENTORS

Alex Anvari
Alpine Race Coach, Stratton Mountain, VT

Fabio Biondi
Researcher and Director of the Operational Cyber Int. Course, NATO CCDCOE

Lindsay Blount
Project and Business Manager, Military and Veterans Affairs, William & Mary

Eric Brown
Senior Research Scientist, Global Research Institute, William & Mary

Chris Burdett
Assistant Professor, Department of Political Science, Virginia Commonwealth University

Michael Dick
Visiting Professor of Practice, Lewis B. Puller, Jr., Veterans Benefits Clinic, William & Mary Law School

JD Due
Executive Director, Center for Military Transition, School of Business, William & Mary

Robin El Kady
Data Scientist, Information Environment Assessment Team,
Public Diplomacy Division, NATO Headquarters

Amy Ertan
Cyber and Hybrid Policy Officer, NATO Headquarters

Kay Floyd
Director, Whole of Government Center of Excellence, William & Mary

Dr. Kira Graves
Director of Critical Thinking Enterprise, G-2, U.S. Army Training and Doctrine Command

Christine Hines
Vice President for Artificial Intelligence, Analytics and Automation, Man-Tech

Vladimíra Hladíková
Assistant Professor, Faculty of Mass Media Communication, University of SS. Cyril and Methodius

Margaret Hu
Professor of Law and Director, Digital Democracy Lab, William & Mary Law School

Anna Hurajova
University Lecturer and Researcher, University of SS. Cyril and Methodius

Kathleen Jabs
Special Assistant for Military & Veteran Affairs, William & Mary

John G.L.J. Jacobs
Director, Atlantic Forum

Bernie Kaussler
Professor of Political Science, James Madison University

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

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

Elizabeth Losh
Professor, American Studies, William & Mary

Oana Lungescu
Principal Spokesperson, NATO Headquarters

Trish Martinelli
Executive Director, Defense Entrepreneurs Forum

Keith Masback
Owner & Principal Consultant, Plum Run LLC

Robert McMath
Senior Analyst, Information, Intelligence, Cyber, Electromagnetic Warfare, and Space (I2CEWS) Operations and Technologies, Janus Research Group

Ben Miller
CWMD & CBRNE Senior Manager, Defense Mission Area, Noblis

Dobril Radoslavov
State Expert, Defense Policy Directorate, Ministry of Defense, Bulgaria

Paula Redondo
Programme Officer for Russia and Central Asia, Public Diplomacy Division, NATO Headquarters

John Ringquist
Senior Defense Officer/Defense Attaché for Angola and Sao Tomé and Principe, United States Army

David Rowe
Fulbright NATO Security Studies Scholar and Visiting Fellow, German Marshall Fund

John Scherpereel
Professor of Political Science, Coordinator of the Modern European Studies Minor, James Madison University

John Scott
COO and President, Ion Channel

Chris Shenefiel
Adjunct Lecturer, Applied Cybersecurity, Computer Science Department, William & Mary, Security Research Principal Engineer, Cisco Systems

Daniel Shin
Cybersecurity Researcher, Center for Legal and Court Technology's (CLCT), William & Mary Law School

Dr. Anthony Stefanidis
Professor of Computer Science, William & Mary

Dr. Elis Vllasi
Lecturer, Simon Fraser University and NATO Field School

Jonathan Ward
Retired U.S. Diplomat, U.S. Departments of State and Commerce

Anna Wheeler
Strategic Initiatives Lead, Leidos

Roger Yee
Managing Partner, Outcome/One

PARTNERS

NATO
OTAN

WMGIC
GLOBAL INNOVATION CHALLENGE

WILLIAM & MARY
REVES CENTER FOR
INTERNATIONAL STUDIES

WILLIAM
& MARY
CHARTERED 1693

WHOLE OF GOVERNMENT
CENTER OF EXCELLENCE

WILLIAM & MARY
LAW SCHOOL

DISINFOLAB

PART II:
Agenda and Case Study

WMGIC x NATO Countering Disinformation Challenge Event Schedule

21st October 2022

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

Opening Address by Baiba Braže
Assistant Secretary General for Public Diplomacy, NATO

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

Sophie Workinger
Global Innovation Challenge (WMGIC)

Dorothy Gao
Global Innovation Challenge (WMGIC)

Mel Onwusika
Global Innovation Challenge (WMGIC)

Aaraj Vij
DisinfoLab

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 . 1:15 - 2:00 P.M. E.S.T.

Keynote Address - General Philip M. Breedlove (USAF, Ret.)
Former Commander, Supreme Allied Command, Europe, SHAPE, Belgium and Headquarters, U.S. European Command, Stuttgart, Germany

Oana Lungescu
NATO Spokesperson

Closing Remarks from NATO - Christine Del Bello
Special Advisor to the Assistant Secretary General Public Diplomacy Division (PDD), NATO

Kathleen T. Jabs
Special Assistant for Military & Veterans Affairs, William & Mary

Case Document for Undergraduate Teams, Mentors, and Judges

OVERVIEW

The WMGIC x NATO HQ Countering Disinformation Challenge consists of seven 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. 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 disinformation. 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.

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), and

C) 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 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 ET) to the deadline (11:00 am ET) to work on their project and create all deliverables.

DELIVERABLES

Submit a five-slide maximum PowerPoint/PDF slide deck including a slide with a 150-word project summary. Teams also have the option of creating content (such as an infographic or meme) although there will be no penalty if not accomplished. Please submit the presentation by 11:05 am ET.

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 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.

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 2 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.

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 5 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 or "quack" 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. NATO has prioritized countering disinformation through "pre-bunking," such that the Alliance can inoculate civilians to misleading information before it proliferates online. However, the challenge of developing comprehensive and coordinated responses to disinformation persists for NATO.

The case documents below offers 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 STREAMS

ARTIFICIAL INTELLIGENCE

Objective: How can NATO member nations limit the spread of disinformation in the event of a targeted and widespread Artificial Intelligence (AI)-driven campaign?

Overview

Artificial Intelligence (AI) by machines or computing programs seeks to emulate human intelligence to perform tasks. AI has a variety of applications in speech recognition, linguistic translation, visual perception, and decision making. Contrary to what its name suggests, AI is not a form of conscious intelligence but rather the result of training models with large quantities of data. In the age of Big Data, AI algorithms can process increasingly large datasets to identify patterns and replicate them with a greater degree of accuracy.

Recent improvements in AI have enabled the mass production of social media posts, images, audio, and video content that appears to be human or made by humans. While these tools are not intrinsically harmful at the individual level, widespread use by nations and ideologically-driven organizations poses a threat to international security. Disinformation campaigns by adversarial actors may be significantly more harmful to the information ecosystem given the scale and speed at which AI-generated content can be produced and weaponized.

Further, efforts by governments and technology companies to combat disinformation are limited, and have been insufficient at addressing disinformation in its current state. The lag between disinformation dissemination and developing disinformation solutions makes it difficult for states and individuals to take preemptive action against targeted campaigns.

Background

AI technology has developed rapidly over the last decade. AI has unique potential for disinformation based on the way it is designed – models are trained on large datasets using different algorithms to prime the AI for future scenarios. Over the last decade, an increase in the quantity of available data, the development of new machine learning algorithms, and the deployment of more powerful Graphical Processing Units (GPUs) has vastly improved AI's capabilities. These new capabilities have huge ramifications for the weaponization of disinformation. Given the speed and relative accuracy of certain emerging AI systems, malicious actors are quickly gaining the ability to create automated disinformation attacks at a large scale.

NATO recognizes these emerging threats and is following a number of initiatives to combat AI-powered disinformation. Among these include NATO's support for the development of more powerful sentiment-based analysis algorithms to detect problematic emotionally charged posts online. Given the tendency for these kinds of posts to gain traction, it is vital for NATO and its members to have access to this technology. This further aligns with NATO's desire to maintain its technological edge over China and Russia, two countries known for spreading disinformation in several NATO member countries.

NATO has also supported the use of AI to combat disinformation. Models have been developed that can detect whether text has been generated by a human or an AI, whether an image has been altered, or whether a piece of audio was synthetically generated. Utilizing AI to protect NATO countries' information spaces is vital to building and maintaining civil cohesion.

Big Events

AI is an incredibly dangerous tool for disinformation campaigns because of the speed and sophistication of content produced. NATO has previously investigated GPT-2 and GPT-3, which are two examples of powerful AI language model systems. GPT-2 can summarize, translate and read text, while GPT-3, the most advanced version of these models, has the ability to write essays and produce syntactically correct code. These language models from OpenAI have huge implications for disinformation. The speed and sophistication at which both systems can regurgitate information is cause for alarm because it has proven the ability to produce disinformation at a quicker rate than other AI. Additionally, GPT-3 has been found to reinforce specific biases and stereotypes towards minority groups, which further exacerbates the language model's ability to cause harm if leveraged by a malicious actor.

Beyond the invention of AI tools that can spread disinformation, NATO has also identified the Kremlin's use of bot and deep fake accounts on a variety of social media platforms to target users in several Western Balkan nations to spread propaganda regarding vaccines and Russian military might. Both deepfakes and emergence of language processing systems demonstrate the power disinformation and AI have when combined.

Current Solutions/Failures

Disinformation produced by AI can be combated through both technical and non-technical means. To distinguish computer-generated content from human- produced text, AI-based tools can analyze textual content and automatically detect cues such as word patterns, syntax construction, and readability. AI companies, such as Google, Facebook, and Twitter, are currently developing more robust vetting algorithms to prevent the spread of false information. However, algorithms such as these have been accused of online censorship.

NATO has proposed several recommendations for mitigating the spread of disinformation, including active moderation of bias-laden phrases and slowing the total amount of output social media companies are able to produce in times of political chaos. Instituting these measures will contribute to a safer online space that is ready for the next generation of AI-powered tools. Such measures have proven difficult to implement; large social media platforms like Facebook and Twitter have little incentive to manually slow the amount of content posted on their respective platforms.

Furthermore, NATO has supported the practice of social media companies having in-house fact-checkers to prevent false information from spreading. Human fact- checkers or moderators are able to perform the primary research required for verifying the authenticity of a report or an image. Additionally, Facebook, YouTube, and Twitter provide their users with the option to report other users suspected of spreading false information, whether knowingly or unknowingly. While fact-checking and reporting content is valuable, neither are able to stop a piece of disinformation from spreading rapidly when the content is first posted.

Advances in AI may revolutionize the way how the world both consumes and combats disinformation. While the prospects are exciting, these changes should be for the better. In the fight against disinformation, crowdsourcing of collaborative knowledge among professional organizations is crucial to verifying raw information, while informed communities can contribute to ethical monitoring activities.

CLEAN ENERGY

Objective: How can NATO member nations find and combat clean energy disinformation in order to reduce their carbon emissions– especially if the disinformation is spread by influential corporations?

Overview

Clean, or renewable, energy is generated from recyclable sources and does not emit greenhouse gas. Common forms of renewable energy are solar, hydro, tidal, wind, and geothermal; nuclear, although it is not renewable, is considered clean energy. Biomass energy, which generates power by burning organic materials, is considered renewable because it releases significantly less greenhouse gasses than the burning of fossil fuels.

Why does renewable energy matter? The world is facing one of the most significant crises of our time–climate change–and nowhere on Earth is left untouched by its effects. While shifts in temperature have occurred throughout human existence, global temperature has increased dramatically since the 1800's due to human activities, such as burning fossil fuels to create electricity. These fossil fuels release greenhouse gasses, trapping heat from the sun and creating an increasingly hot planet. The Global Energy and CO2 Status Report found that the power sector generated almost two-thirds of global fossil fuel emissions, with China, India, and the United States responsible for 85% of the net increase in emissions in 2018. The sudden increase in temperature causes food and water insecurity, displacement of populations, economic disruption, increased conflict and terrorism, ocean acidification, and increasingly extreme natural disasters. A solution to mitigate the detrimental effects of climate change lies in the switch from fossil fuels to renewable energy, although clean energy disinformation hinders progress.

Background

Humans have long relied on energy for survival. Resource depletion, scarcity, cost, technological advancement, and quality push humans to search for alternative sources, including the current push towards renewables. Although renewable energy was only popularized in the 20th century with the commercialization of wind turbines, the use of clean energy is not a new phenomenon. The waterwheel, for instance, was used as early as the first century BCE in the Middle East. A rudimentary form of the windmill originated around 600 CE, and early solar energy was used in France in the 1860s. While clean energy has been around for millennia, it was not until the discovery of the harmful effects of carbon emissions, and the advent of international agreements like the Kyoto Protocol, that countries began investing in fossil fuel alternatives. In 2021, NATO met with the Executive Director of the International Energy Agency (IEA) to discuss climate change, climate security, the transition to clean energy, and strengthening cooperation between both organizations. NATO leaders plan on incorporating climate change counter measures into every aspect of NATO's work, and the IEA will spearhead countries' efforts to switch to clean energy and reach net zero emissions. Additionally, NATO aims to reduce CO2 emissions by 35% within the next decade, and be fully carbon neutral by 2050. Steps towards these goals involve emergency preparedness, researching the impacts of pollution, reducing the military's carbon footprint, and improving energy efficiency.

However, as governments transition away from fossil fuels, opposition to the movement grows. The economies of oil producing countries, such as Saudi Arabia, Russia, and the United States, rely on fossil fuel exports, and the goal to reach net zero carbon emissions by 2050 would lead to a 75% plunge in net revenues. Because of that, oil producing countries are more reluctant to transition to clean energy, and fossil-fuel companies utilize disinformation and propaganda to limit support for change. These global corporations have historically "downplayed and distorted" evidence of climate change, and its link to their products, as early as the 1950's. By spreading false science and propaganda, companies aim to confuse the public and policymakers to thwart protective climate action. Now, large corporations turn to greenwashing to manipulate consumers. Additionally, a large portion of clean energy disinformation is found on, and spread through, a particularly dangerous platform–social media. In a short period of time, "false, misleading, and questionable information" can be spread to a large audience. As the world fights to prevent the devastation that would accompany a 1.5 ° C temperature increase, stifling clean energy disinformation has never been more crucial.

Big Events

Germany faced multiple cases of disinformation about clean energy in 2021. First, an Australian Facebook user shared a meme containing a picture of solar panels covered in snow with text saying "Germany's green energy FAIL." A different meme shared within the same week shows "stagnant" wind turbines and a caption that reads "COAL plants to the RESCUE...!" A few weeks later, the posts had been viewed over 60,000 times. Both memes falsely indicate that clean energy does not work and that Germany had to "return" to coal. However, the drop in energy production is expected during winter months. Furthermore, one image was of Russia, not Germany, and the claim of thousands of wind turbines not moving was linked to a known climate change skeptic blog. Data from German renewable energy sources at the time prove that there was never a time, even during the storm, that energy production halted.

Another instance of clean energy disinformation comes from ExxonMobil, one of the world's largest international oil and gas companies. In fall of 2021, ExxonMobil paid for at least 350 advertisements intended to influence proposed legislation in New York state that aimed to block the future use of natural gas in new buildings. By claiming that being "forced" to switch from natural gas to electric would "could cost you more than $25,600," ExxonMobil increased resistance to the proposed pro-environment legislation. Meanwhile, ExxonMobile's ad featured wind turbines that the company financed in Canada, misleading consumers about its credibility through greenwashing.

Current Solutions/Failures

Some social media giants have taken initiatives to combat climate change disinformation. For example, Twitter has employed a strategy known as "pre-bunking" to tweak its algorithms to direct users toward credible information before they encounter disinformation. Facebook also announced that it has started to attach warning labels to certain contents and redirect some users to its "Climate Science Information Center" containing accurate information. However, a report from a watchdog group found that Facebook had in fact "failed to label" half of the posts that lead to climate denial. The UK Parliament has drafted the Online Safety Bill specifically aimed to address climate change disinformation. Other NATO countries have also proposed to increase regulations on the issue, but concerns about free speech, as well as practical difficulties fact-checking mass information on social platforms, have hindered attempts to address disinformation through legislation.

Community engagement is another essential tactic clean energy developers employ to counteract disinformation while locating new wind and solar projects. The United States Department of Energy has been outreaching to more local communities about inaccurate ideas surrounding utility-scale solar and wind, especially on its human health and environmental effects. Nevertheless, they have received more pushbacks than in the past given communities' increasing suspicions of renewable energy.

CLIMATE SECURITY

Objective: How can NATO member countries and allies identify and combat climate security disinformation, especially from industries and influential figures, in order to support protective climate policy?

Overview

Climate change, the gradual change of the natural environment observed through temperature, weather, and other natural processes, is a fast growing concern around the globe for the dangers it presents to communities and the environment as we know it. These dangers, spanning from increasing storm intensity to higher transmissibility of certain illnesses, are known as climate security, or the dangers that come as a result of climate change. Despite 97% of experts agreeing that the climate is being altered by emissions, climate change remains politically disputed. Climate disinformation has a long history, and continues today through scientific misrepresentation and nonrepresentational arguments. Consequently, it has been difficult to pass climate policy that will adequately address climate change.

Background

Disinformation about climate change, intended to dispel the belief in climate security, has existed for as long as industry and individuals have understood the harms of production and their actions on the environment. For over 50 years, tetra-ethyl lead was used in gasoline, despite multiple scientific studies about its pervasiveness in the environment and its harmful effects to the human body. Yet, the United States' government looked the other way, claiming that the research should be done by the industry most concerned with tetra-ethyl lead and gasoline. As a result, a single laboratory headed by Robert Kehoe was conducting multiple studies that suggested that the lead was not as dangerous as the above scientific studies were claiming. These studies, heavily cited by policy, the government, and the public as evidence that lead did not pose such a serious problem, were unsurprisingly funded by companies such as General Motors, DuPont, and Ethyl, and later confirmed to be flawed. After 50 years, the government eventually did recognize the danger of lead, and the lead in gasoline was banned fully in 1986 by the EPA. Algeria was the final country to ban the use of lead in gasoline final in 2021.

Today, industries manipulating public opinion continues with "greenwashing," where major companies brand themselves as part of the climate solution—despite actively lobbying to undermine existing regulations.

The degradation of scientific consensus is evidenced by comments by former United States President Donald Trump, "[the Paris Accords] was a terrible deal for the United States. If they made a good deal ... you know with having to do with trade, there's always a chance we'd get back. But it was a terrible deal for the United States. It was unfair to the United States." Internationally, the head of the World Bank dismissed climate concerns, while climate change activists hammered nations such as Sweden for lacking bold policy, and continental reliance on fossil fuels reached unprecedented highs as a result of badly managed energy dependence decisions, showing disinformation and slow progress to be an international issue.

Big Events

In the past few decades, governments around the world have come together in an attempt to create policies and protocols that will curb emissions and mitigate climate change. One of the first major policy initiatives the international community passed was the Kyoto protocol— a treaty created in the 1990's which would hold developed countries accountable for lowering their emissions with the goal of lowering global greenhouse gas emissions. Disappointingly, due to fossil fuel companies pushing "uncertain science" agendas and focusing attention on the omission of developing countries, the protocol failed to take root.

This pattern follows over subsequent years and many other attempts throughout the world to pass climate legislation. Furthermore, many of the policies that do get passed are subject to the ideals and actions of the following leaders, evident by the deviation of Trump from the climate initiatives put forth by the Obama Administration. From policies to international treaties, the work that is done can and has been undone by political figures who prioritize industry over fighting climate security.

Current Solutions/Failures

NATO addresses climate security with many initiatives, particularly the Science for Peace and Security (SPS) Programme, the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and their Trust Fund projects. Through these, NATO prioritizes international cooperation in support of many countries' efforts to address climate security, aids emergency response preparedness to climate disaster events, protects energy security and promotes energy efficiency, develops climate policy and standards for member states, and much more.

Another major international undertaking is the Paris Agreement, or Paris Climate Accords. The main goal of the Paris Accords is limiting the mean global temperature increase caused by global warming to no more than 2 °C, or 3.6 F. It also aims to strengthen each country's response to climate change and shift finance flows in a way that mitigates greenhouse gas emissions. In order to reach these goals the Accords declares the use of "appropriate mobilization and provision of financial resources, a new technology framework and enhanced capacity-building," and "an enhanced fi transparency framework for action and support." At signing, the treaty included 55 countries and accounted for 55% of the total global emissions. Today, 194 countries have signed the Accords.

Bearing in mind the progress made, understanding and fighting climate security remains central to the survival of communities globally. Countries must fight, domestically and internationally, against climate disinformation and in support of effective climate policy.

PUBLIC HEALTH

Objective: How can NATO member countries and their allies counter disinformation in the public health sphere?

Overview

Disinformation in public health is a growing crisis worldwide. The World Health Organization defines public health disinformation as "false or misleading information in digital and physical environments during a disease outbreak." It is a coordinated or deliberate effort to gain money, power, or reputation. For example, some sources of disinformation argued that COVID-19 was nothing more than a "little flu" and encouraged people to openly flout norms like social distancing, promote unscientific treatments like ivermectin, and question the scientific validity of vaccines. It is a broad topic that can cover anything from vaccine efficacy, severity of disease. Public health disinformation can undermine confidence in health authorities that can dampen the state public health response, increase risk-taking behaviors that harm health, and intensify or lengthen disease outbreaks. NATO has publicly rebuked COVID-19 disinformation by Chinese and Russian backed disinformation campaigns, but little progress has been made in actually countering the disinformation.

Disinformation in health has the potential to end the lives of those who choose to believe in the falsehoods and can exacerbate the spread of pandemics like COVID-19. A recent study showed that even brief exposure to

COVID-19 vaccine misinformation made people 6.5% less likely to want a COVID-19 vaccine.

In recent years, the advent of social media has exacerbated the problem of disinformation. Disinformation is spread on these sites because it is framed in sensational or emotional terms. Some have also argued that social media algorithms that promote controversial topics are to blame. Regardless of its source, there is an imperative to stop health disinformation and its damaging effects.

Background

Disinformation in public health is nothing new, with the first organized anti-vaccine group, the National Anti- Vaccine League, appearing in 1866 after Britain's government tried to mandate smallpox vaccines. Many messages that emerged from the group, including the idea that getting sick is part of God's plan and fear of the contents of the vaccine, are currently being used by anti- vaccine groups today.

The modern anti-vaccination movement can be traced back to Andrew Wakefield's now discredited paper in the Lancet that suggested a link between the Measles, Mumps, and Rubella (MMR) vaccine and autism. Despite the retracement of the paper by 10 out of the original 12 co-authors and the Lancet journal itself due to evidence that Wakefield falsified and ignored contradictory data, committing several ethical violations, the paper is used as justification by several anti-vaccination advocates.

Wakefield's paper served as the catalyst for increasing health disinformation all around the world. In South Africa, "AIDS denialism," a false belief denying that HIV causes AIDS, was adopted at the highest levels of the national government, reducing access to effective treatment and contributing to more than 330,000 deaths between 2000 and 2005. In 2019, the United States saw multiple declarations of public health emergencies due to measles outbreaks and in Europe, the World Health Organization revoked the measles eradication status of Albania, the Czech Republic, Greece, and the United Kingdom.

Big Events

The COVID-19 pandemic has highlighted the urgency to tackle public health misinformation. From the earliest days of the pandemic, disinformation spread over the source of the virus and how it was spread to its severity. Once patients ended up in the hospital, disputes over treatment occurred. And when vaccines became widely available in Spring 2021, some refused to take them due to being influenced by misinformation. Several groups have been responsible for spreading this disinformation.

A European Anti Vaccination group known as "V_V", active in France and Italy harassed doctors, vandalized government buildings, and disrupted vaccination campaigns. Despite several accounts linked to the group being banned from Facebook and other social media platforms, V_V continues to spread anti-vaccination information and has branched out to include anti-democratic and climate change denial messaging.

In December 2020, a lab in Egypt published a study from a randomized clinical trial that claimed that the drug ivermectin was 90 % effective against COVID-19. However, the paper was not peer reviewed and several researchers found major issues with the study, including plagiarism and ethical issues. Despite these concerns, worldwide interest in ivermectin grew and several figures promoted it as a treatment against COVID-19 and equivalent to a vaccine. In Slovakia, the health ministry allowed the use of ivermectin against COVID-19 and the Czech health ministry approved doctors prescribing ivermectin at their own discretion. This caused a false sense of security and instead of helping patients, it instead led to increasing complications due to the drug's side effects.

Current Solutions/Failures

Community engagement is an important protection against health disinformation. Governments have attempted to institute evidence based programs designed to help students identify disinformation and educate students on proper scientific practices. The US Department of Health and Human Services issued a tool kit to educators in an attempt to incorporate information on countering disinformation into the classroom. This is an attempt to solve the root cause of disinformation and prevent people from believing false information in the first place.

Additionally, health professionals play a role in combating health disinformation. Taking the time to engage patients and the public on disinformation can help address the lack of health literacy that leads to disinformation. Several clinicians have gone on social media to counter disinformation and have partnered with community organizations to create centralized, clear public health messages. Disinformation is able to thrive because of mixed messaging from public health professionals. A lot of the initial sources of disinformation have come from studies that have evaded replication and are able to bypass the traditional peer reviewed process and gain a larger audience.

The main challenges faced in addressing public health disinformation include the lack of communication between different social media networks over problematic users, the ability to evade content moderation, and its sheer scale. Several social media platforms have engaged in content moderation and have banned accounts that promulgate disinformation, but new users and content pop up faster than they can be moderated and deleted.

Overall, several attempts have been made to counter public health disinformation, but none have been completely successful. NATO's current approaches have included identifying the sources of disinformation and how digital platforms influence operations. There is a need for innovative, fresh approaches to tackle this national security problem

RUSSIA-UKRAINE WAR

Objective: What are ways NATO member states and allies can combat the Kremlin's false narratives about the war in Ukraine to prevent the manipulation of public opinion?

Overview

Russia has weaponized disinformation domestically and internationally for decades. The Kremlin creates and spreads false narratives to manipulate populations, attempting to establish their role as a global leader and undermine NATO influence. Since Russia's interference in the 2016 US elections, NATO countries have recognized the benefits of combating Russian disinformation because of the rapid spread of harmful narratives like the betrayal of the West. Russian disinformation falsely pushes the myth that Russia is a victim, and Western countries are aggressors which has intensified during the war in Ukraine. Additionally, the open information space in Western countries allowing debate to take place puts Russia at an advantageous position to influence decision making. In wartime settings, Russian disinformation acts as a weapon to divide societies by causing chaos and deepening polarization, while promoting internal support for the Kremlin regime.

The Kremlin's robust disinformation strategy, known as the "Firehose of Falsehoods" model, is rapid, continuous, and repetitive, pushing false and misleading information through a variety of mediums. These include state owned media channels, domestic activists, internet bots, and fake social media accounts. The high saturation of Russian disinformation undermines the freedom of the information sphere in NATO countries and creates a perception of authenticity. During the war in Ukraine, Russia has been committing horrific atrocities against innocent civilians, while utilizing disinformation in Ukraine and abroad justifying Russia's actions. These narratives villainize Ukrainians, aim to destroy Ukrainian national unity, and strive to manipulate the perception of Russia's invasion among NATO countries. In this wartime setting, Russia is using disinformation as a weapon to assert power and dominance.

Background

While Russian nationalist propaganda targeting Ukraine existed pre-Cold War, modern disinformation emerged during Russia's invasion of Ukraine in 2014. The invasion was triggered by Moscow's growing uneasiness about Crimea becoming more closely aligned with Western institutions, especially with the EU and NATO. Russia's claim that Ukraine was part of Russia, the "one nation" myth, and historical revisionism about the history of Ukraine's statehood were the central tenets of Russian disinformation during the annexation of Crimea.

The Russian government and state-controlled disinformation outlets pushed this false rhetoric in Eastern Ukraine, resulting in substantial local support for the Russian military troops in the area. The reports employed fear mongering tactics about "nazi-fascists" hiding within Ukraine to justify the military presence. The residents of the peninsula, many of whom were Russian speakers, were convinced that it would be safer and better for the country if Crimea came back under Russian control. Many officials believe that without the months-long Russian state media campaigns supporting the invasion, the annexation never would have succeeded.

Following the annexation, NATO affirmed Ukraine's sovereignty and stated their goal to support Ukraine's ability to provide for its own security through political and practical support. Cooperation between Ukraine and NATO deepened following the invasion. According to the organization, NATO has been "actively countering a significant increase in disinformation and propaganda" since the annexation. Despite Ukraine's membership hopes being stuck in limbo for years, on September 30, 2022, Ukrainian President Volodymry Zelenskyy officially applied for an "accelerated accession" for Ukraine to join NATO.

Big Events
In the leadup to the February 2022 invasion, Russia used television networks like RT and Sputnik, and social media sites like Telegram and Twitter, to spread nationalist rhetoric, delegitimize Ukrainian rule, and undermine NATO unity. Prior to the invasion, Russia accompanied its military operations with influence campaigns to reduce international support and destabilize Ukrainian leadership. Putin claimed the attack was to "demilitarize and denazify" the Kyiv regime to justify his imperialist actions. Some other pro-Kremlin narratives claim Ukraine's army staged attacks to gain global support, Zelenskyy faked public appearances, and Ukrainian refugees committed crimes in foreign countries.

Russia has used several strategies for spreading these false narratives, including hacking into Ukrainian networks, impersonating Ukrainian columnists on social media, and using bot accounts with AI generated faces. An altered video of Zelenskyy telling the Ukrainian military to stand down also spread on Ukrainian media, creating uncertainty within the country. Russia has also created 'clones' of popular media sites filled with false information and "sleeper sites" that slowly gain followers through innocuous posts before switching to propaganda, both in an attempt to spread pro-Russia narratives more discreetly.

The scale and varied techniques used by Russian actors create a complex and unpredictable influence operation, posing a significant challenge to Ukraine and its allies.

Current Solutions/Failures
Since the war in Ukraine began in February, Ukraine has demonstrated resilience to Russian disinformation. However, Russian narratives continue to manipulate people's opinions in Ukraine and abroad. Russia's aggressive information warfare strategies will continue to evolve and adapt, putting Ukrainian national unity and NATO democratic institutions at risk. NATO's approaches, although partially successful, lack coordination and flexibility.

Currently, NATO emphasizes proactive communication to identify disinformation, a strategy known as "prebunking." This approach consists of rapidly reacting to disinformation by publicly communicating the truth before the false narratives can manipulate public opinion.

In 2021, NATO developed their Toolbox for Countering Hostile Information Activities. It established a model to respond to these activities by understanding, engaging, and coordinating to help develop future courses of action. NATO IS staff also meet regularly to brief on Russian disinformation activities and provide guidance and funding to strengthen member state resilience to disinformation.

Despite these efforts, NATO member states lack a consistent and flexible response to Russian Disinformation. Western states approach and implement solutions differently based on various factors, such as history, culture, education, media quality, and relationship to the Russia regime. According to the former Director of NATO Information Office Moscow, Amb. Tomasz Chłoń stresses that a coherent NATO response should focus on "(i) their civic resilience, (ii) their offensive capabilities as much as their defensive ones and (iii) minimizing the differences in how individual Western countries approach disinformation in practice."

NATO can also learn from the various ways in which Zelenskyy has combated Russian disinformation during the war. As part of an offensive strategy, Ukraine has been borrowing from the Russian playbook by countering disinformation with a plethora of truthful information. On platforms with large Russian speaking audiences such as VK, the Ukrainian media highlights Putin's war crimes. This offensive method allows Zelenskyy to bypass Putin's state-controlled propaganda aimed at painting Russia as the "good guy" in the war.

Ukraine has also been fighting Russian disinformation by showcasing Zelenskyy's digital following and emotional appeal to the Ukrainian people. He has used his charisma and public image to keep pro-Ukrainian sentiment strong online, fighting Russia's attempts at fracturing the nation's unity. The robust, emotional online action has likely played a large role in thwarting Russia's attempts to destroy Ukrainian morale during the war. NATO countries can use this method to gain back the populace.

Media literacy education programs are another method of improving a population's resilience to disinformation because they arm people with the tools needed to identify and counter false narratives by assessing information online. NATO funds efforts to boost disinformation resilience in member states; however, more emphasis can be placed on this subject. Media literacy includes thinking critically about content in the media and considering its influences on thoughts and behaviors.
Global big tech companies like Facebook and Twitter have attempted to reduce disinformation on their platforms. Users can also report and debunk

fake posts to draw attention to fake sources like Russian bots. Although NATO buckling down on content shared on these platforms is an effective way to identify suspicious posts, these efforts often involve different legal complications in different NATO member states. Additionally, despite moderate regulations in recent years, disinformation continues to infiltrate the internet because of the Kremlin's innovative strategies.

SEXISM & GENDER-BASED VIOLENCE

Objective: What are ways in which NATO member nations and allies can tackle sexism and gender-based violence disinformation?

Overview

The following case explores how disinformation is used to perpetuate stereotypes or beliefs about women that increase sexism and amplify gender-based violence. Gendered disinformation is used as a tool to target female politicians and activists, with campaigns aimed at undermining their competence and attacking their personal characteristics. Various international agencies and state bodies have recognized that sexism and gender-based violence disinformation is harmful to women and prevents us from achieving gender equality. Despite various policy actions by NATO member states and widespread calls for change, the public is seeing increased prevalence of the perpetuation of negative stereotypes about women, gendered attacks on women, and false statements surrounding gender-based violence. These disinformation media campaigns are often used as a basis for harmful behavior and misogyny in real life, which can be violent and lead to further marginalization.

Background

Sexism is any form of prejudice or discrimination against an individual on the basis of their sex or gender. Women are the predominant victims of sexism. Gender- based violence (GBV) is defined by the United Nations as any act of violence that results in or is likely to lead to physical, sexual or psychological harm or suffering to women. Sexism and gender-based violence disinformation is used to promote misogynistic narratives about women, as well as undermine their competency. This form of disinformation is most commonly used as a tactic against prominent women in politics and activism.

Online communities have been instrumental in giving a voice to female activists against oppressive governments by facilitating organization of Women's Marches and amplifying their #MeToo stories. However, social media platforms are also responsible for enabling the spread of sexist disinformation. Over 90% of the women in the Global South interviewed by the Economic Intelligence Unit have experienced gender-based disinformation attacks online. Gendered disinformation campaigns are often waged against female political candidates, with 41.8% experiencing some form of sexual harassment and taunts online. Women hold only 24.3% of parliamentary seats around the world, which demonstrates the barriers in place to restrict female political participation. Russia, Hungary, and Brazil are all examples of countries that have witnessed the use of sexism disinformation in political campaigns to quiet female opponents.

Gender inequality is still a major problem. The World Economic Forum estimates that at our current pace it will take more than a century to achieve gender equality. Now more than ever, the internet shapes our views and beliefs and is the biggest source for obtaining information upon which our views are based.

Big Events

Germany's elections in 2021 for the Office of the Chancellor demonstrated the impact of sexist disinformation and its negative repercussions for women trying to enter the political sphere. Annalena Baerbock was the Green Party's candidate for Chancellor and the major target of Russian-backed online disinformation campaigns. She faced several attacks, with 18 of the most shared posts about her on Facebook containing false or misleading information about her. Baerbock appeared to have been attacked more than her male counterparts, with her attacks trending more personal. Another example of harm caused by sexism and gender-based violent disinformation comes from Iran, where women's rights activists have received online threats of violence and other forms of hate speech. Facebook has been the primary home of these coordinated attacks against Iranian feminist groups. Additionally, in 2017, Rwandan presidential candidate Diane Kwigara was the victim of fake nude photos spread on the internet to destabilize her campaign. These are just a few of the myriad examples of sexism and gender-based disinformation in action.

Current Solutions/Failures

Germany has adopted the world's strongest law against online hate speech and harassment - the Network Enforcement Act (NetzDG). Unfortunately, this regulatory change has not been enough to prevent sexism-related disinformation and indicates that more innovative solutions are needed. NATO's Women, Peace and Security unit is working to ensure that all member states are actively pursuing policies to further gender equality and has instituted gender advisors across all of NATO's military structures to move forward their goal of greater integration of female perspectives. More should be done to explore how NATO and its members can monitor public messaging about women and prevent disinformation.

Proposed solutions to tackle sexism and gender-based violence disinformation include developing gender-sensitive digital literacy policies and practices. These initiatives have yet to receive widespread backing to make implementation feasible and effective. Social media companies are yet to be held accountable for their role in allowing harmful disinformation to spread. The Biden-Harris Administration in the United States has recently launched the "Global Partnership for Action on Gender-based Online Harassment and Abuse," which aims to bring governments, nonprofits and the private sector together to solve the growing issue of "technology-facilitated gender-based violence.” The organization acknowledges the need for greater documentation of gendered disinformation, particularly regarding hate speech and online gender-based violence. This information can allow us to better identify trends and prevent issues from spiraling out of control.

TERRORISM

Objective: How can NATO member states and allies prevent the spread of disinformation by terrorist and extremist groups?

Overview

Extremist groups have spread disinformation with the goal of promoting recruitment and misleading the public. Since the advent of the internet and mass communication, terrorist groups have had a mostly unregulated and widespread platform to disseminate lies and disinformation with the dual-headed purpose of cleaning up their image and winning support. Now, experts and world leaders are trying to combat and prevent the dangerous tendrils of terrorist disinformation from doing more harm.

From jihadist groups located in the Middle East to racial supremacy groups in the NATO Alliance and partner nations, terrorist and extremist organizations take to the internet and social media platforms to spread their misguided ideals. In the wake of attacks in Europe and elsewhere, the Islamic State in Syria, commonly known as ISIS, managed to recruit upwards of 4,500 citizens from countries such as the United States, United Kingdom, Germany, and other NATO member nations. Much of this was done through the spread of disinformation online. By taking advantage of popular platforms such as Twitter, Instagram, and Facebook, these groups disseminate lies regarding the perfect utopia they plan on establishing. They also broadcast videos with the intent of glorifying their efforts, leading the isolated youth of the developed world to find themselves relating to and justifying terrorism.

Background

Disinformation and false justification by extremist groups have been increasingly problematic in the digital age. ISIS is a notable group that employs the internet for their outreach and spread of ideology. At the height of their efforts and physical strength in 2014-2015, ISIS had a digital footprint of around 50,000, to 90,000 accounts on Twitter openly advocating for or being closely aligned with the group. With the numerous accounts targeting citizens and young adults across the NATO alliance, this threat is not unique to just one nation. There are similar cases across not only mainstream and somewhat regulated internet platforms, but also on less regulated applications, such as Telegram, which is end-to-end encrypted. In the United States, for example, the spread of disinformation has led extremist groups such as the Oath Keepers, 3 Percenters, and the Boogaloo boys, to see a steady rise in membership. Groups such as these are emboldened and strengthened by the increasingly divisive political climate resulting in a precarious security situation around the globe.

Big Events

By using fast and effective mass communication, extremist groups commonly target young adults who have grown up online. Back in 2012, two Norwegian citizens carried out a plot to bomb a newspaper that had, by Al-Qaeda's rhetoric and standards, represented the Prophet Mohammed in an insulting light. These foreign born citizens had been first contacted and then indoctrinated by Al-Qaeda. While the plot to bomb the newspaper company was foiled, there was the potential for a mass casualty event targeting civilians sparking concern regarding terrorists' use of the media to spread disinformation. In 2004, the extremist, separatist organization, Euskadi Ta Askatasuna (ETA), bombed the train station in Madrid killing and wounding approximately 2,000 civilians. ETA waged a campaign of violence for decades, utilizing the spread of disinformation to gain new members and win support. New Zealand also faced a terrorist attack in March of 2019, where an extremist fatally shot 51 people in separate mosques. This occurred in Christchurch all while being streamed live on Facebook. The man, Brenton Tarrant, wrote "The Great Replacement," a racist manifesto brimming with threats to minorities and plans of "replacing'' different cultural, ethnic, and racial groups. The manifesto is a sombering example of the spread of disinformation, and the attack is a horrific example of its repercussions. The use of Facebook to disseminate both the manifesto and the livestream points to the need for solutions to prevent the spread of purposeful lies and harmful ideologies.

Current Solutions/Failures

With social media channels being a primary route for the spread of disinformation, companies are taking a larger role in combating extremism and false claims. Twitter, most notably, has taken one of the clearest steps to curb this spread of disinformation, with their "Birdwatch Feature." This feature allows regular users to add "notes" to other people's tweets, which helps flag content that is clearly disinformation or seeks to spread or incite violence.

However, as social media companies become more effective at curbing extremist rhetoric, terrorists locate new platforms to use. In the last two years, as right-wing extremism has drastically risen in many countries, Twitter began taking drastic measures against inflammatory rhetoric. Now, the messaging service Telegram, has exploded in popularity. With an addition of 90 million accounts in the span of one month, the end- to-end encrypted application seems to have undone much of the progress made against online disinformation.

With the rise of end-to-end encryption applications, the simple regulation of popular social media platforms is only a band-aid solution. While one may suggest the outright banning of these applications altogether, it comes at the cost of taking away the tools of repressed citizens and ideals of free speech.

WMGIC & NATO Countering Disinformation Challenge 2022: Partnering to Change the World

Kate Hoving, *W&M News*

"This is serious work at a serious moment."

Teresa Longo, Associate Provost for International Affairs and Executive Director of the Reves Center, set the tone for the day in her introductory remarks.

On October 21, 2022, the Reves Center was headquarters for the William & Mary's Global Innovation Challenge (WMGIC) x North Atlantic Treaty Organization (NATO) Countering Disinformation Challenge. More than 400 students from across the NATO Alliance and Partner Nations participated in his historic competition. This was the second year of the challenge, and the interest in combatting disinformation across NATO countries was even more pressing, not just because of Russia's invasion of Ukraine.

"The aim of disinformation is not to convince anyone; it is to confuse you to divide you, to ultimately make you unable to take decisions, and to make us unable to take decisions together. That's why it's really important that we are all working together against it," NATO Spokesperson Oana Lungescu explained. "This is not just about us at NATO HQ. It's about everybody, and it refers to disinformation from Russia but also from China, and from state and non-state actors. We now see a worrying convergence between disinformation from Russia and China but also between anti-vaxxers, for instance, and those who oppose Ukraine's rights to defend itself."

Everyone – from opening and closing speakers to the participants – understood and focused on the urgency of harnessing WMGIC's approach to bear on current issues.

Above: Teresa Longo (Credit: Tyler Lawrence); Below: Oana Lungescu

General Philip M. Breedlove (USAF, Ret.), Former Commander, Supreme Allied Command, Europe, SHAPE, Belgium and Headquarters, U.S. European Command, Stuttgart, Germany, delivered the Keynote Address, "Countering Disinformation: Russia's Hybrid War and the Information Battlefield." Breedlove had visited Ukraine just before the invasion. "I am pleased that you are looking at this important task of countering disinformation – of hybrid or grey war.... I'm really proud of what you're doing, and I'm really looking forward to hearing your ideas. And more importantly, I hope what we will see is our nations' putting your ideas into practice."

In her opening address, Baiba Braže, Assistant Secretary General for Public Diplomacy, NATO, remarked that she also was looking forward to the teams' "very creative but also very rational results."

She went on to give the students their mantle: "All our futures, as individuals as well as societies, but also of the Alliance, are very much in your hands. You are the future of NATO."

BUILDING ON PREVIOUS SUCCESS

The William & Mary Global Innovation Challenge (WMGIC) is a student-led organization that hosts premier case competitions. These events champion interdisciplinary collaboration and mobilize young adults to tackle global issues. Established in 2017, WMGIC provides undergraduate students worldwide a platform for open collaboration and discussion with peers, faculty, and knowledgeable professionals to analyze and create sustainable and scalable solutions. The competition increases students' knowledge about the case study, design thinking, holistic sustainability, innovative processes, and policy entrepreneurship. The WMGIC philosophy is that students have creative perspectives on important issues, and the challenges are a chance to showcase their ideas. When the first William & Mary's Global Innovation Challenge (WMGIC) x North Atlantic Treaty Organization (NATO) Allied Command Transformation (ACT) Cybersecurity Challenge was held in November 2021, the organizers and participants were thrilled that 56 teams from 52 universities competed in 7 streams. It was the largest challenge WMGIC had hosted and the first time WMGIC had partnered with Whole of Government Center of Excellence and NATO ACT. Despite the months of planning and preparation, no one knew if it would attract a diverse group of participants, and if NATO ACT would find the partnership of value.

However, the response was so positive and the projects so innovative, that planning for the next yearwmgic worker started almost as soon as the hotwash was completed.

Above: General Philip M. Breedlove (USAF, Ret.); Below: Baiba Braže

But as always with a successful debut comes the worry that it cannot be maintained, much less topped.   Also, because WMGIC is a case competition hosted by undergraduate students there is turnover in leadership as seniors graduate and freshmen join.

In 2022, could they maintain the high standards and numbers of teams?

Well, the WMGIC x NATO Countering Disinformation Challenge 2022 exceeded expectations in every possible way. Participants numbered in the four hundreds, with more than 100 registered teams of students across 9 streams from more than 50 universities from 13 NATO partners countries participating– from Romania to Columbia; Turkey to the U.S. (William & Mary had a team, NATO Your Business, which was part of the Foxtrot Stream.)

Teams were assigned one of seven topics: Russia-Ukraine War; Public Health; Climate Change: Clean Energy; Climate Change: Climate Security; Artificial Intelligence; Gender-Based Violence; and Terrorism.

They received their case competition briefing document several days prior to the event.

For seven hours, the undergraduate student teams worked with mentors to refine their presentations addressing counter disinformation in one of seven realms, each competing to develop the most comprehensive and innovative – as well as practical and achievable – solutions. Each plan of action needed to consider NATO’s existing capacity and the actions NATO should implement within the next 12 months.

The thirty-nine mentors and judges represented a wide variety of backgrounds and experience inwmgic workingwmgic member working government, industry, academia, and other disciplines.

Mentors rotated through several university teams to give expert advice, offer feedback, and answer questions. Judges evaluated the presentations on the following criteria: feasibility & effectiveness, creativity, privacy, sustainability, and fiscal pragmatism.

The panels of judges evaluated the proposals and selected one winning team from each stream for a total of nine winners, who received $500 each. The winners were announced at the conclusion of the Challenge via a live Zoom event/webinar. The team solutions will be published by NATO in the spring.

COMPETITION WINNERS

- ALPHA STREAM: University of North Georgia - University of North Georgia - USA
- BRAVO STREAM: Javelin - King’s College London - UK
- CHARLIE STREAM: NSF Team - University of Alberta - Canada
- DELTA STREAM: Dukes for Defense - James Madison University - USA

- ECHO STREAM: VU-Waseda Team - Vrije Universiteit Amsterdam - Netherlands and Germany
- FOXTROT STREAM: Enssat - ENSSAT Lannion - France
- GOLF STREAM: ICP FOR NATO - Institut Catholique de Paris - France
- HOTEL STREAM: RMCC - Royal Military College of Canada - Canada
- INDIA STREAM: Not NAFO - George Mason University - USA

All presentations are available online.

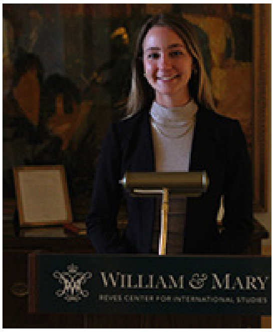
COLLABORATING FOR A HOPEFUL FUTURE

The intensity of the challenge--working together and competing in a set amount of time across time zones and international boundaries, with influential mentors and judges you have never encountered –makes for an exhilarating day. But Longo had put the day's excitement into a larger context as she addressed the student teams, mentors, judges and sponsors.

"The [WMGIC student team members] have been mentored by the director of our Whole of Government Center of Excellence and supported by the Reves Staff. As a result of their education at the university, they are prepared for the work," Longo said. "I believe this is also true for all of you who are in the competition--one where collaboration is key. Collaboration means that you will learn from each other and from your mentors. All of this is possible because of the collaboration of the university and NATO headquarters' public diplomacy team. We are building a transnational partnership that looks to the future and to the role of all of you will play in a peaceful world."

The students approached the collaboration and potential will the same note of optimism, sensitive to both their mission and their mandate.

"As the world increasingly looks towards technology for solutions to global challenges, understanding the dangers it poses is crucial." said Sophie Workinger, WMGIC director of operations & development. "By uniting not only undergraduates, but also mentors and judges, this challenge helps bridge the gap between students and professionals. I am incredibly proud of the WMGIC team for breaking world records with this monumental event, and I am looking forward to continuing WMGIC's goal of amplifying the voices of the next generation of creative problem solvers."



Lungescu said, "We are all in a way information defenders and information warriors. NATO is here to defend our right to live as we would wish -- to our freedom our democracy our values -- and I'm really energized by the fact that you are all NATO ambassadors. I really count on you to continue doing this work for your future but also for all of us."

Above: Sophie Workinger '24 (Photo Credit: Tyler Lawrence)

One of last year's opening speakers, Kathleen T. Jabs, then-Acting Secretary of Veterans and Defense Affairs for the Commonwealth of Virginia, has in the intervening year has become William & Mary's Special Assistant for Military & Veteran Affairs. In 2021 she delivered her opening comments remotely via Zoom, but this year, in her new role, she was able to deliver her remarks at the closing session in person in the Reves Room.

"We are so proud at William & Mary to host this event where we have an opportunity to encourage students to think boldly and act humanely... a powerful example of what happens when you harness intellectual energy to confront the most pressing issues of our times."

Jabs continued, "The presentations I listened to were compelling and rigorous and left me full of hope and optimism that the students here now in this room and around the world will continue to partner to change the world."

Above: Kathleen Jabs; Below: WMGIC 2022 (Photo Credit: Tyler Lawrence)

This event was organized by the W&M Global Innovation Challenge and the North Atlantic Treaty Organization, with support from the DisinfoLab, Whole of Government Center of Excellence, Reves Center for International Studies, and William & Mary Law School. W&M thanks the American Academy of Diplomacy for its assistance.

The videos of the winning presentations as well as the opening and closing remarks are online.

All aspects of the challenge, including all student pitches, are published by NATO's Cooperative Cyber Defence Centre of Excellence.

Photos above: WMGIC members and volunteers managed the competition from the Reves Center.

PART III:
Winning
Pitches

Winning Pitches

ALPHA STREAM: Russia/Ukraine War
TEAM NAME: University of North Georgia

AUTHOR NAMES: Mohini Devadath, Avery Johnson, Jessica Case, Nathanael Hines, Autumn Coan, Odahia Carrasco Lebron, Gabriella Bartlett, Michelle Borosak, Ella Reid, Gabriela Ocasio, Natalie Pippin

AFFILIATIONS: University of North Georgia

SUMMARY: The primary objective satisfies the need to combat disinformation by granting Ukrainian citizens Internet access, via NATO-funded satellites to prevent the spread of further conflict into NATO Member States and Kremlin pushed disinformation. The satellite will be funded via the Innovation Fund which provides monetary backing for DIANA inventions and is modelled after SpaceX's Starlink satellite, which utilizes cybersecurity measures. This benefits all NATO members against potential cyber-attacks.

The secondary objective, or VPNs, grants citizens within the Russian Federation access to worldwide internet and broadband for accessing non-state-funded applications and media sources, wherein citizens may disseminate accurate information about the war. While Russian citizens may not access the VPN for information contradicting state-run media, there is a high possibility there will be exposure to activism initiatives on the conflict. With both objectives taken into consideration, disinformation can be combated on the ground and at the source.

BRAVO STREAM: Terrorism
TEAM NAME: Javelin

AUTHOR NAMES: Oliver Rooney, Paul Gers, Rafaël Thibaut, Lorenzo Tual, Alexandre Doré, Simon Holin, Baaz Chandwan, Antonio Macedo, Devan S. van der Poel

AFFILIATIONS: King's College London

SUMMARY: The fundamental danger of misinformation spread by terrorist groups is the exploitation effect it has on existing vulnerabilities within NATO member states. To tackle the rise of disinformation within member-states concerning terrorism, we recommend the establishment of a working group within the Doctrine, Concept and Experimentation branch of the NATO Strategic Communications Centre of Excellence. This specialized section will be dedicated to the analysis of each state's vulnerability to disinformation and to creating practical policies to suppress and eliminate the threat. For each nation the response will be weighted by a Dis-information Resilience Framework. This working group would be financed by 1% of the Civil Budget and hosted within the infrastructure of NATO's Strat Com.

The long-term objective of this projection is a doctrinal change in the logic of NATO to counter disinformation; adopting a tripartite approach consisting of understand, engage, and an additional objective of redress.

CHARLIE STREAM: Gender-Based Violence
TEAM NAME: NATO Field School SFU

AUTHOR NAMES: Hailey Lothamer, Keiren McClelland, Kenzie Ekkebus, Guneet Pooni, Jonathan Reep

AFFILIATIONS: Carleton University, University of British Columbia, University of the Fraser Valley, Dalhousie University, University of Alberta

SUMMARY: There are three distinct categories of this plan: education, cooperation, and training. Training focuses on using existing assets, in particular course programs at the NDC, to provide comprehensive gender perspective instruction. It seeks to involve female leaders, past and present, to introduce positive, step-oriented goals to reinforce the commitment to and necessity of fair treatment in NATO. It also highlights the liabilities of unaddressed sexual violence and gender discrimination disinformation.

Cooperation focuses on the support offered by third party and private sector actors while emphasizing core values of democracy, cooperative security,

human rights. It encourages all member nations to participate in creating a forum for dialogue on gender misinformation, involving academia and private firms.

Finally, this plan seeks to implement policies and practices of digital literacy across the alliance focused on information campaigns about the role of women in holding government offices, participating in the economy, and voting in elections.

DELTA STREAM: Climate Security
TEAM NAME: Dukes for Defence

AUTHOR NAMES: Isabelle Klein, Ethan Rothstein, Alida Schreuders, Sebastian Bienkowski, Brianna Scherb

AFFILIATIONS: James Madison University

SUMMARY: Countering climate security disinformation, and disinformation in general, has to speak to younger generations. We have developed a plan to combat this issue with the use of diversion, re-direction, and education. Grabbing the attention of an audience is the first step in educating them. Disinformation is spread largely through media platforms, as internet trolls attempt to sway individuals away from valid information in the interest of personal gain.

Our plan is to troll the trolls. Using software such as Information Discovery that sifts through information on the basis of validity, we propose that NATO follows posts containing misinformation with a meme. These memes will grab the attention of the audience and following the post, provide the viewer information educating them on the threat of climate security and its impact on domestic and international communities.

ECHO STREAM: Clean Energy
TEAM NAME: VU-Waseda

AUTHOR NAMES: Jan Kersten Otte, Ivo Andriessen, Thomas Swelheim

AFFILIATIONS: Vrije Universiteit Amsterdam

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.

FOXTROT STREAM: Artificial Intelligence
TEAM NAME: ENSSAT

AUTHOR NAMES: Julien Thomas, Laurian Bertrand, Quentin Bultez

AFFILIATIONS: ENSSAT Lannion

SUMMARY: The ever-increasing computational power enables more means to produce disinformation, mainly through Artificial Intelligence, such as deep fakes. Social media such as Facebook and Twitter are already facing this issue and developed their own solution, but a "closed", proprietary solution can lead to issues such as one entity having full control over information and censorship.

Our solution would be a browser extension that acts similarly to an ad blocker. Given a piece of information, an AI trained with users' feedback will be able to identify it as disinformation and block/hide it.

The first key principle is transparency, we want our algorithm/AI to be transparent, everyone should be able to understand why a piece of information was considered disinformation.

The second key principle is crowdsourcing, with fact checkers acting as ombudsmen in case crowdsourcing can't find a consensus.

GOLF STREAM: Public Health
TEAM NAME: ICP for NATO

AUTHOR NAMES: Noah Martin, Vincent Savary Jackson, Erwan L'Hereec

AFFILIATIONS: Institut Catholique de Paris

SUMMARY: The idea is an AI algorithm capable of identifying potential disinformation in social media content. It would be formed using deep learning and databases of official public NATO health documents. It then scans through content emitted on social media platforms and flags those of high or almost certain risk to be official public health forgeries. The algorithm then records it and compiles a database of threats it publishes daily.

Disinformation threats classified as immediate risk lead to pop-up notifications alerting a team of analysts who then confirm the risk/deny it and submit reports to NATO governments or allies. This enables NATO to make more cost-effective and optimized public health counter-disinformation campaigns countering emerging social media threats. Such information can also further public research and discourse on the issue.

HOTEL STREAM: Russia/Ukraine War
TEAM NAME: Royal Military College of Canada Model NATO Team

AUTHOR NAMES: Richard Sun, Nick Hao, Liam Brown

AFFILIATIONS: Royal Military College of Canada

SUMMARY: Goal: NATO will launch a social media campaign designed to suppress Russian false narratives and boost NATO's public perception within the targeted country by preempting negative Russian narratives with positive NATO narratives.

- **Action 1:** Assist communities in member states at the Eastern edge of the alliance or otherwise at-risk through infrastructure development, healthcare and education aide, and community outreach;

- **Action 2:** Engage with social media influencers and sponsorships to showcase cutting-edge technology, collective security, and the opportunities that NATO provides to both militaries and civilian citizens of member states through these development and outreach projects;

- **Action 3:** Coordinate with social media corporations to systematically detect, remove, and counteract Russian internet bots;

- **Action 4:** Designate a task force to debunk Russian disinformation on social media within 24 hours of its dissemination, replacing it with positive messaging as outlined.

INDIA STREAM: Terrorism
TEAM NAME: Not NAFO

AUTHOR NAMES: Andrew Wright, Drew Kolber, Marshall Yaffe

AFFILIATIONS: George Mason University

SUMMARY: The Technology Trust for Terrorism Prevention (3TP) is a fund created to aid in the prevention of online disinformation. In providing access to financial support, 3TP incentivises communication organizations to establish good governance policies, target hubs of misinformation, and try to rectify or ban such channels. This will then extend to communities that opt-in to this program where they can report points of concern that arise, allowing the fund to tackle the issue alongside community leaders, school districts, and religious institutions. Communities and organizations involved will receive certification for their involvement This is targeted initially at mid-level organizations as they are most inclined to ensure their platforms are a safe space for users. The fund will ensure the spread of disinformation is significantly reduced and cannot spread within communities and cause harm.

PART IV:
Other Pitches

CCDCOE

All Pitches

ALPHA STREAM: RUSSIA/UKRAINE WAR

TEAM NAME: Refreshers

AUTHOR NAMES: Alex Lipniski, Charlotte Sutton, Sandra Tkacz, Hamish Langley, Tom Randle, Nimrah Farooq, Jake McEvoy, Tom Binch, Conrad Sullivan, Oliver Williams

AFFILIATIONS: Nottingham Trent University

SUMMARY: After having noticed the ideological constraints within Russia, our group has collaboratively proposed the solution of utilising social media spaces as a cost-effective way of mitigating the spread of disinformation. Considering factors such as effective budgeting and cost, as well as sustainability and impactfulness, the most efficient approach within the media industry as a short-term solution is to fund Ukrainian journalism and private Russian journalists. This initiative would start immediately and span over the next 12 months. As a result, this will diminish disinformation within Russia by establishing NATO's objective aims of unity and solidarity. Leading on, our next approach is to work collaboratively to expand partnership with industry to expand cyber security. In the long-term this will increase our external defences, re-enforcing internal cyber security and protecting ideals of freedom of speech and democracy.

TEAM NAME: Cherwell & Common Ground

AUTHOR NAMES: Ella Myers, Isobel Cook, Christina Herold, Gideon Futerman, Julia Bator, Conrad Lam, Maria Rotaru, Jemima Storey, Ariana Minea

AFFILIATIONS: University of Oxford

SUMMARY: A working group will be created that brings together NATO in conjunction with private and public organisations across civil society, technology, education, and politics. As a multi-organisational working group, we will be able to provide a neutral force behind tackling disinformation, which will enable collaboration between different bodies. We have identified three key approaches to target different forms of disinformation. We will build strategic networks by; establishing a conference bringing together public and private sector actors to discuss policy methods, as well as a research network. We will combat social media disinformation by; providing easy-to-digest tip sheets on how to combat disinformation online and adapting Covid-disinformation strategies to this scenario. We will build target grass-roots level media by providing toolkits to regional authorities and maintaining local media autonomy.

TEAM NAME: PSSA

AUTHOR NAMES: Ali Mostafa, Sama Elmahallawy, Farah Swellam, Mai Ghoniem, Mariam Salem, Kenzy Masry, Miriam ElSebai, Loren Emad Morgan, Ahmed Amer, Ingie Gohar, Malak Talat, Omar Mohanna

AFFILIATIONS: The American University in Cairo

SUMMARY: Despite Ukraine's resilience, Russia's multidimensional strategy for spreading false narratives around the involved stakeholders in the conflict is still a problem. Thus, using NATO's innovation fund and previously developed initiatives to combat disinformation like pre-bunking, we aim to carry on a media literacy project that tries to allow proactive thinking from citizens in face of emotional triggers. It also tries to utilize the journalists and other important influencers that they generally do not use like influencers in sports. The main implementation will involve applying VR headsets in NATO HQ and these headsets should stimulate real-time interaction with news that makes employees fight disinformation. In addition, we also include for long-term the development of application that sends alerts to citizens about fake news and update the citizens after fact-checking the news. In doing so, the project should not be limited to NATO-allied countries, but it should spread to non-NATO countries as well.

TEAM NAME: KBIR

AUTHOR NAMES: Yidi Zeng, Shirui Wang, Yufan Chen, Xingyi Chen, Ziyi Zhao, Xiang Fang, Yiran Wang, Yiming Chen, Sirui Gao, Zhaoxin Li, Zheng Chen, Tingke Yang, Muwei Jiang, and Nanqiao Deng

AFFILIATIONS: Keele University

SUMMARY: NATO disinformation Office functions as a department to reduce disinformation emerged during Russia-Ukraine war from both short term and long term. In short term, the office will cooperate with social media and use AI as a tool to end disinformation. However, there is still some information that cannot be recognized by AI. Therefore, long-term measures will also be launched. The office intent to use all possible media (short videos, social medias) to spread some intermedia such as documentary which tells the facts and make use of celebrities to expand the influence. By implementing these two operations, NATO could minimize the spread of disinformation by Russia and make the truth heard by the general public.

TEAM NAME: NATOx

AUTHOR NAMES: Alex Garcia, Rosie Wrigglesworth, Thomas Britton, Ozan Somyurek, Tymoteusz Syrytczyk, Catherine Brewer, James Melia, Niki Kiiskinen, Turner Ruggi, Iñigo Bailon

AFFILIATIONS: University of Oxford

SUMMARY: Our guiding principle is to combat impersonal disinformation with personal information; to set the agenda rather than constantly defend. We want authentic connections between NATO citizens and Ukrainians, and emotional responses to tackle mass apathy- Russian disinformation is dispelled by citizens' contact with truth.

We will use video since it is most effective for cross-platform diffusion across social media. Emotional, 'human interest' content similar to Hunter Prosper's "Stories from a Stranger", alongside semi-comedic collaborations between regionally specific influencers and Ukrainians will enable NATO citizens to hear real stories directly from those affected; NATO can facilitate these projects and assist creators in publicising and spreading the finished product.

We will trial this approach in NATO's eastern flank, due to their latent potential for sympathy with Ukrainians and experiences on the frontline of Russia's disinformation. After twelve months the project will upscale to other affected regions, ensuring a tailored approach to specific cultures.

BRAVO STREAM: TERRORISM

TEAM NAME: Pre-emptive Strikers

AUTHOR NAMES: Ekrem Kaan Afşar, Ecem Naz Demirkaya, Toprak Sezgin, Fatma Beyza Güler, Shukria Malek Zada, Aykut Küçükyıldız, Deniz Tetik, Alkım Özkazanç

AFFILIATIONS: Middle East Technical University

SUMMARY: The North Atlantic Treaty Organization (NATO) is working to prevent the spread of disinformation about terrorism. NATO shall counter the terrorists' usage of religious and cultural pretexts to legitimize their actions while also promoting humanitarian conduct while handling terrorists. NATO should work with the European Union (EU) to adopt the Rapid Alert System (RAS), which is a digital platform that allows EU member states and EU institutions to share information about disinformation and coordinate responses. NATO shall also work with the Group of Seven (G7) to defend democracy and prevent the spread of disinformation. NATO shall coordinate collaboration with the United Nations Information Centres (UNICs), which have country-specific experiences and could provide mechanisms that NATO lacks to counter disinformation about terrorism. NATO shall work with the UNICs to form mechanisms such as "fact-checking partnerships" to effectively target radicalization and recruitment propaganda and promote such ventures accordingly.

TEAM NAME: Security and Defence Club UNAV

AUTHOR NAMES: Jairo Císcar Ruiz, Paula Las Heras Martiricorena, Sara Hernández Calabrés, Jesús Rizo Ortiz, José Antonio Latorre, María Álvarez, María Martín Andrade

AFFILIATIONS: University of Navarra

SUMMARY: Under a five-point plan, the proposal is to boost the capabilities of NATO to reach a larger public, consolidate its public image, cooperate with the EU, and bolster ties with private industry contractors.

First, to create a Joint Disinformation Center, funded by NAC, that will act as a coordination cell group for intelligence agencies across Member States and provide feedback.

Second, to launch a public campaign on social media to reach a larger public, with the double purpose of expanding the knowledge on NATO and discrediting terrorist and extremist messages.

Third, to strengthen collaboration with the EU through sustained dialogue and increased engagements.

Fourth, to collaborate with private industry, enhancing programs with entities specialized in intelligence and monitorization.

Finally, to attract and engage with civil society, private entities and particularly the youth to reinforce the understanding of the organization and promote its values and principles.

TEAM NAME: Serious Candidates!!

AUTHOR NAMES: Jack Page, Sri Lanka, Oliver Mofardin, Isha Kayani, Dan McIlroy, Zeph Rubins, Kat B, Jake McAteer

AFFILIATIONS: Nottingham Trent University

SUMMARY: Two-pronged strategy to enhance and improve NATO's current anti-disinformation framework

1. Build response capability

- Entire NATO alliance needs to have no chinks in the armour, only as strong as its weakest member
- Create and share a common toolkit for all NATO members to facilitate, using methods devised by combined NATO groups
- Online Extremist Internet Disinformation task force: independent centre not dissimilar to the CCDCOE, which will recruit pre-existing analysts and specialists from all member states, thus keeping within current budget requirements for 2022/23

2. Individual Education

- Enhance NATO's online public resources, assisting not only military, but by default the civil issue of disinformation and extremism – important as grassroots disinformation weakens the respective nation's military
- Regular distribution of NATO intelligence/information packages to the media, helps to "pre-bunk" disinformation

TEAM NAME: Team Sashimi

AUTHOR NAMES: Clarissa Lilananda, Melvin Leong, Sean Woon, Roisin Alice Mary Hogarth, Caitlin Hayley Susanto, Daryl Lim Kai Wen, Aryan Sanghrajka

AFFILIATIONS: King’s College London

SUMMARY: Counterterrorism operations have traditionally utilised kinetic capabilities. However, the foundation of terrorism is only undermined by detecting and disrupting radical narratives. ACTIC serves as a joint platform to sense-make disinformation narratives and connect NATO member states (NMS) to share information, training, and best practices.

ACTIC’s Information-Fusion Team provides a common protocol for NMS to voluntarily share unprocessed intelligence on emergent disinformation narratives. They will collaborate with external organisations to acquire more information and insights. Analysed information is disseminated to NMS.

ACTIC’s Joint-Training Team invites mid-career intelligence professionals to undergo training in information operations best-practices. They are also kept up to date with the latest trends in disinformation narratives. Classes will also be incorporated into existing tri-service CPXs for inter-service learning.

ACTIC’s Research & Development Team works with research institutions and think tanks to analyse latest disinformation trends and generate policy recommendations.

CHARLIE STREAM: GENDER BASED VIOLENCE

TEAM NAME: Hermits

AUTHOR NAMES: Katie Rey, Ethan Cohn, Julia Bahadrian, Elliott Thimonier, Jules Roger, Ryotaro Muroya, Borja de Pedro Sarasola, Elham Khosravipour

AFFILIATIONS: Edinburgh University

SUMMARY: Creating a NATO Information Neutrality Committee (NINC) that would develop policies and legislation for member countries to follow and adopt, establishing a united strategy against terrorist disinformation. Based on the creation of mini-publics in members states that define boundaries for the a NATO council to formulate policies to counter disinformation leading to terrorism. These policies would be then taken to each member states, allowing discussion of modifications in each country and reaching a personalised policies, following NINC guide-line, that would be strongly recommended to impose in each country. We have provided a sample of potential policy proposals that the NINC could recommend.

TEAM NAME: University of Edinburgh

AUTHOR NAMES: Adith Srinivasan, Luisa Langmann, Narek Nahapetyan, Christina Yuen, Elizaveta Belkina, Jerry Li, Tushar Aneja

AFFILIATIONS: University of Edinburgh

SUMMARY: Disinformation from terrorist and extremist groups poses a threat to national and international security due to its potential to influence and radicalize vulnerable groups. This is exacerbated particularly by the "echo-chamber" dynamics of social media algorithms. As such, NATO is recommended to set up a 'Civil Society Advisory Panel on Disinformation and Counterterrorism' in cooperation with the Committee on Public Diplomacy (CPD). This multilateral forum should promote civil society engagement and the cooperative, bottom-up creation of social media content to act as a counterweight to disinformation. Furthermore, this proposal can be regarded as an initial step within a longer-term strategy. It helps build public diplomacy momentum for the pursuit of a Joint Statement within the North Atlantic Council to make tackling misinformation a national. Additionally, it builds public and political pressure to address the dissemination of disinformation and echo-chambers algorithms through industry-level change.

TEAM NAME: Claras + 1

AUTHOR NAMES: Vladimíra Martínková, Clara Marie Engelsleben, Clara Müller-Sohnius

AFFILIATIONS: Vrije Universiteit Amsterdam

SUMMARY: Gender-based violence through misinformation needs to be recognized as a stand-alone issue threatening digital civic society. Our initiative will be proposed to Meta as they dominate the digital space, and they need to improve their image.

The project deploys two channels: AI and individual reporting. The combination of both allows a holistic approach to identifying and labelling gender-based violence. The consequences are two-fold. Firstly, labelled content is downgraded by the algorithm with the intent of decreased visibility to both the general public and the victims themselves. The second effect is a social one in terms of awareness-raising and offering support to the victims. Individual reporting allows for feedback to be given and shared on a separate Instagram account, if consented to. The feedback loop can be used to measure engagement with and the success of the project.

TEAM NAME: Istanbul Bilgi University Team

AUTHOR NAMES: Nisa Selin Akıncı, Yeliz Kıroğlu, Syed Mustafa Iqbal

AFFILIATIONS: Istanbul Bilgi University

SUMMARY: We aim to create a digital tool for children aged between 10-15. According to us, gender-based issues create an internal security problem because it causes great difficulties in ensuring the safety of a certain part of the population. This application we aim to create will target children whose ideas can be challenged based on unproblematic ways to solve gender-based issues, and it will consist of educational activities. It will also include a glossary that addresses gender stereotypes and sexist discourses and aims to change them. We believe that creating a digital literacy and education tool for children in this age group can influence their opinions. We believe that gender-based issues are mainly political because there is not much effort put into challenging them by certain governments. Especially, in Turkey after the withdrawal from the Istanbul Convention. An educational tool is a need for solutions to this issue.

TEAM NAME: Potential Solutions

AUTHOR NAMES: Mariam Saleh, Saisha Ahluwalia, Advait Shanker

AFFILIATIONS: University of Toronto Mississauga

SUMMARY: We must recognise that gender-based violence disinformation is not just exacerbated through a lack of accountability and willingness on the part of social media platforms but is also the result of deep-rooted misogynistic attitudes that allow for such disinformation to be prevalent. Additionally, cultural and political differences across NATO member states may further complicate efforts to address these challenges at an IGO level. As a result, we propose that the NATO Committee on Gender Perspectives formulates a digital literacy programme to disseminate in schools and workplaces that challenges misogynistic attitudes and helps individuals in NATO states be more critical on how they interact with information in the digital space. We also propose that the Committee works with the Gender Balance and Diversity Task Force and Diversity and Inclusion Programme to ensure that as many voices from across countries, cultures and gender identities are included to enhance the programme's reach.

TEAM NAME: The Best Team

AUTHOR NAMES: Karla Ranjeva, Sol Herrera Penido, Cecilia Mangherini, Chanda Lesa, Lou Rameau

AFFILIATIONS: University of Kent

SUMMARY: We highlighted the role of disinformation in sexism and sex-based violence, by offering three solutions to tackle those problems. Two are short-term, while the last one is long-term and attempts to solve the problem at its core. Creating an accord between governments, NATO and media outlets, we limit the amount of 'fake-news' that will reach the public. Moreover, the implementation of a credibility software conjointly with financial penalties would prevent the spread of unverified information. Finally, engaging children in researching sexism and the value of fact-checking will raise their awareness on social issues in order to develop their critical thinking and hence, transform the status-quo. This would be a long-term solution; however, it would be necessary in order to truly diminish disinformation concerning sexism and gender-based violence.

TEAM NAME: University of Surrey

AUTHOR NAMES: Ellen Parry, Henry Arnold, Libby Taylor, Abean George, Alisha Khan

AFFILIATIONS: University of Surrey

SUMMARY: We are pushing a 2-pronged approach that tackles misinformation in the context of SGBV as a specific supplier/consumer issue in the arena of social media.

Approach one emphasizes the protection of social media consumers through the use of a specialized social media filter which builds upon Germany's NetzDG. Our approach differs because flagged misinformation content is not deleted immediately, rather an extra disclaimer is attached preceding the post providing the consumer with context and a further chance to avoid the post if desired.

Approach two targets the future producers of social media misinformation via early education. A NATO produced curriculum with emphasis on SGBV misinformation would be readily made available to all member states to incorporate into existing curricula. Key pillars of this curriculum would include, internet awareness, the role of social media filters and a remodelling of sex education to include more about consent and violence.

DELTA STREAM: CLIMATE SECURITY

TEAM NAME: (L)IES UOM

AUTHOR NAMES: Stavros Piperidis, Myrsini Salasidou, Angelos-Rafail Naskidis

AFFILIATIONS: University of Macedonia

SUMMARY: "Indicate the fake." Our proposal addresses disinformation on climate change and security issues by focusing on the "bad actor" and the aspect of internal and external key stakeholders. The first recommendation focuses on public diplomacy. Concerning internal action, we propose the creation of a software and a unique methodology that allows the collection and interpretation of quantitative and qualitative data, like research or social media posts, RStudio. Regarding the external action we propose a digital campaign that supports independent users to identify, and address verified instances of disinformation. The second recommendation refers to the Mas-

tering NATO's know-how in CCS efforts. Internally, NATO should provide a platform that facilitates sharing of Allied information and data in relation to Climate Change & Energy. NATO should pursue coordination efforts in terms of CCS and lead by example, aiming to establish a global network that works as a first defence against disinformation.

TEAM NAME: Cyberian Huskies

AUTHOR NAMES: Grace Johnson, Dylan Watson, Julia Bowen, Britney Tran, Yvonne Gymiah

AFFILIATIONS: University of Texas at San Antonio, University of Texas at Austin, University of Texas at Arlington

SUMMARY: In order to aid states in assessing disinformation risks as it relates to climate security, members will be provided with media oversight from the NATO Stop Light Initiative. The NATO Counterfeit Collaboration using keyword scraping, independent verification requests, and prioritization of certain industries will be composed of subject matter experts and members of the IPCC. The NATO Stop Light Initiative's Media Task Force will utilize aggressive media campaigns based on the analysis and verification from the Counterfeit Collaboration team. These media campaigns will discredit misinformation about climate security and promote verified content. In addition, quarterly reporting by the Media Task Force will promote transparency in the processes through press releases that cite consistently verified industries and influencers. Overall, nation-states will contribute funding for this Initiative towards facilities, task force employees, media implementation, liaison partnerships, and keyword scraping resources.

TEAM NAME: Perception

AUTHOR NAMES: Zeynep Özdemir, Tuna Taşır, Arda Öke, Abdulfatah Eskangi

AFFILIATIONS: Middle East Technical University, Dokuz Eylül University, Bilkent University, Doğuş University

SUMMARY: NATO has to focus on strengthening the public interest to counter disinformation. This could be done by forming a unit that will be in close contact with the civil society. We propose forming a unit under NATO that will not only train NGOs, municipality, and city councils, they will also form a relationship with the universities through student clubs.

TEAM NAME: Team MDX

AUTHOR NAMES: Dev Engineer, Suhaib Shaukat, Opemipo Babatunde

AFFILIATIONS: Middlesex University

SUMMARY: We are focusing on how we can deal with the issue of climate security within the existing framework that is designed by NATO. We suggest introducing three initiatives; Climate Assure, Ask NATO and Étude et recherche. Climate Assure or Climate for All is a reliable research team focused on curating, researching, and presenting generally disputed facts concerning climate security across all social media platforms. This team will drive regular online campaigns, enhancing discussions surrounding climate security while maintaining an open channel called Ask NATO where all climate related questions can be answered, and discussions can be initiated. We strongly believe in inoculating members of the public against disinformation through proactive information sharing dissemination and demystifying the subject of climate security. And lastly, Étude et recherche which translates as study and research, in which a syllabus is designed to study disinformation as a subject across different member states.

TEAM NAME: University of Toronto

AUTHOR NAMES: Vismay Buch, Asima Kidwai, Akshita Sangha

AFFILIATIONS: University of Toronto

SUMMARY: It is important to combat disinformation at its roots, hence, we are focusing on combating counterfeit science at its source. We propose to use open source softwares such as Disinformation Index, climate feedback amalgamated with advanced software suit from NATO's cyber command to make a detailed structured list of all universities, scientists, and institutions to flag the publications that contradict fact checked scientific data. Once flagged, NATO's cyber experts at the CCDCOE in Tallinn and NATO HQ in Brussels can act on the disinformation and counter it in cyber domain through the 3 level analysis of credibility, sentiment, and impact. Our plan is fiscally responsible as it uses open-source software and fortifies them with NATO's inhouse Research and Development team.

TEAM NAME: WConsulars

AUTHOR NAMES: Leila Desir, Lindsey Alcy, Amina Loum

AFFILIATIONS: Carleton University

SUMMARY: We propose creating an accessible app that delivers accurate environmental information to the general public. In this app, we will be sharing NATO-approved scientific resources and NATO-funded climate research. The goal is to translate scientific research in a quick, consumable manner. In hopes of addressing climate security, the app will cover the four main elements (i.e. water, fire, earth and air) and space. The app will have two key features: a verification and a main feed function. The verification function allows users to quickly verify information's accuracy and legitimacy based on source credibility and NATO approval. The feed will consist of popular topics relating to each element within the scope of climate security. An individual can freely navigate between elements and related topics through a scroll navigation system.

ECHO STREAM: CLEAN ENERGY

TEAM NAME: Peter Schramm Scholars

AUTHOR NAMES: Adrianne Silva, Noah Harshbarger, Matthew Savage, Robert Mouledoux, David Maloney

AFFILIATIONS: Ashland University

SUMMARY: Our 2-phase approach to countering disinformation includes companies and individuals. The first phase deals with disinformation originating from businesses. NATO has contracts with many companies. If NATO determines a company is spreading disinformation, we propose NATO wean themselves from said company, while turning to others who do not spread disinformation. This would have no upfront costs. The second phase deals with advertising campaigns to disseminate information regarding the benefits of clean energy. We propose the creation of 4 videos discussing Nuclear, Solar, Geothermal, and Wind Energy. These videos would be distributed to the member states and NATO would reach out to localities to create more personalized advertisements. These will increase awareness about the benefits that clean energy without villainizing fossil fuels and provide personal connections between clean energy and individuals.

TEAM NAME: Milestoners

AUTHOR NAMES: Anna Házas, Dominik Benjámin Gulyás, Borbála Kovács, Dóra Tolnai

AFFILIATIONS: Amsterdam University College, King's College London, University of Warwick, University of Groningen

SUMMARY: The main goal of the project is developing critical thinking trough unconventional and innovative action. The most efficient way of changing consumer behaviour is to influence the way the population is receiving this information. This needs to be a bottom-up approach. We also have to build on previous good practices for this. The individual steps need to be a part of a wider campaign. Flagging social media posts for fact checking is one of the vital steps. NATO should be aiming to use the most novel AI technology in flagging and approving the posts. Each nation state should create their own website for reliable clean energy information that can potentially be connected to social media posts. A group of experts and scientists should be assembled to set up a central website that should be further developed and customised on a national level.

TEAM NAME: Kenyon College

AUTHOR NAMES: Ben Gruodis-Gimbel, Griffin Crump, Sally Smith, Nellie Birnbaum

AFFILIATIONS: Kenyon College

SUMMARY: Current means of targeting disinformation are focused on being defensive— it is time to take an offensive strategy. The present narrative around clean energy focuses on climate change as a moral high ground, while we want to redefine clean energy as independent energy. Although misinformation spreads in many domains, social media is oftentimes the doorway for it. With NATO-based tech companies, we can use an algorithm based on Markov's model, allowing us to predict from existing data on users what independent energy campaign would be most persuasive. This lets us tailor the information each user sees based on what the user's primary concerns are probable to be, playing on self-interests. Security threats and independence from non-NATO influences are effective non-climate arguments to reach our target group. Success in this algorithm would have users begin to dismiss misinformation when they see it and lower the odds they engage and spread it.

TEAM NAME: UWE Bristol

AUTHOR NAMES: Ryan Coyle-Larner, Ben Roynon, Isabel Ryall, Megan Say

AFFILIATIONS: University of the West England Bristol

SUMMARY: Proposition - NATO Energy Information Centre
We recommend the creation of a pledge whereby companies take responsibility for the disinformation they disseminate regarding clean energy. Any publication of false information is the responsibility of the signatories either intentionally or by negligence.

Create an arm of NATO to enlist help of academics and students from universities in member nations to identify breaches and keep track of companies who've signed the pledge.

Require representatives of companies to be scrutinised on their contributions to energy information in a specific committee.

The EIC would publish annual reports of those who don't agree to the pledge and who break it. They would be required to publicly apologise and issued fines. We recommend a review of an appropriate fine, potentially similar to the GDPR fine (€10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever is higher).

TEAM NAME: Universidad Santiago de Compostela

AUTHOR NAMES: Fernando Miranda España, Emmanuel Nieto Parodi, Megan Lutch Riveiro

AFFILIATIONS: Universidad de Santiago de Compostela

SUMMARY: We believe that education is key in the attempt to combat and mitigate the effects of disinformation, that is why we consider that all people should be rightly informed regardless of age, socio-economic background, ethnicity, and such.

Our project considers that the best way to fight disinformation is to maintain society informed about clean energy, it makes them less likely to be subjected to propaganda. In order to do so we believe in generating awareness and participation through programmes, platforms and forums is crucial.

We suggest doing this by cooperating with influential actors, such as influencers or renown foundations, and building bridges with NGO's to reach more people and more diversity, with an educational purpose. The idea is to create the means so that everybody can be informed about this topic, this is the only way to have a society capable of identifying disinformation.

TEAM NAME: Georgia Institute of Technology

AUTHOR NAMES: Nora Fahim, Lucas Nahmias, YooNa Weon, Grace Swift

AFFILIATIONS: Georgia Institute of Technology

SUMMARY: Transitioning to clean energy is a paramount security concern for NATO, and disinformation is a major hindrance for countries and companies in their attempts to get buy-in from consumers when they transition to clean energy. As non-renewable energy sources deplete, there are likely to be wars over resources, as well as refugee crises. First, NATO should convene a Climate Summit and agree upon climate "truths," and explain the science and data behind each. They can also implement a public ranking system of countries' military emissions, social media companies' policies, and companies' ads denying climate change. This will educate people about the current climate situation. Next, NATO can use its influence to work with social media companies to implement a circuit breaker system that slows the spread of viral misinformation when they flag a post as gaining too much traction. These solutions will slow the spread of disinformation about clean energy.

FOXTROT STREAM: ARTIFICIAL INTELLIGENCE

TEAM NAME: ROR Syndicate

AUTHOR NAMES: Rares Mihai Bejusca, Roza Maria Pilarek, Oumnia Chaara

AFFILIATIONS: Leiden University

SUMMARY: 1. A web browser extension that scans the social media platform in respect of potential disinformation; underlines the questionable information and links to NATO database^1. The NATO-developed algorithm compares the scanned text with multiple pieces of information on the same topic gathered in the data base and then, based on the probability of the information being true, it marks the information with colours:

- green - close to certain that the information can be relied on
- yellow - not sure/can't determine
- red - if it's close to certain that the text is disinformation

2. The algorithm reports the 'yellow' and 'red' posts to NATO fact-checkers that imitatively verify the text. The fact-checkers also take into account culture, sarcasm, irony etc. Using machine learning the algorithm will constantly learn to verify future posts based on changes made by the fact-checkers

3. The open AI algorithm will be funded by:
   - NATO funds
   - government and local government's donations

[1] The NATO data base:
- gathers articles from reliable sources of information:
- the NATO representatives of each country propose a list of sources of information in their country → NATO appointed committee reviews lists → the articles from accepted sources are gathered in the data base.

TEAM NAME: The Panthers

AUTHOR NAMES: Martin Brown, Luisa Rincon, Carlos Ricaurte, Juan Artunduaga, Josmer Carvajal

AFFILIATIONS: Florida International University

SUMMARY: The Three-Step Action Plan involves three pillars: education, innovation, and application. First and foremost, education is the pillar dedicated to combatting misinformation on an individual level as well as promoting media literacy. Part of our initiative involves fostering the support of local community leaders to aid the educational sector in raising awareness against mass AI-led misinformation campaigns. Innovation involves partnering with the private sector via incentives in the creation of open-source projects, said projects are to be focused on developing an AI system that can automate or flag misinformation content whenever a user browses through them. Application revolves around the application of said open-source tools on major sources through a partnership with NATO. These pillars will end up working under an aligned effort to counter AI-led misinformation by both introducing new projects and creating a stronger general awareness with the hope of being able to counter this growing phenomenon.

TEAM NAME: Keele Ladies

AUTHOR NAMES: Muhan Li, Haoran Zhang, Linyue Xing

AFFILIATIONS: Keele University

SUMMARY: We are SIFTER Project of NATO aiming at Anti-disinformation. Our project is divided in two groups. Firstly, evaluating group. The evaluating group will gather AI experts to evaluate the effectiveness of the major existing disinformation screening mechanisms and will produce reports on those mechanisms. Based on the evaluating report, we will find the most effective existing disinformation detecting system in every specific field (eg. politics field and medical field). For the promotion group, we will promote the importance of anti-disinformation to the public through online and offline ways. The raised public awareness will push the companies to install anti-disinformation system.

TEAM NAME: CGCR Research

AUTHOR NAMES: Matthew Cave, Sonni Dyson, Joseph Enright, Samuel Redding, Ezra Sharpe

AFFILIATIONS: Oxford University

SUMMARY: Approaches to disinformation need to be reconceptualized so that it can be rooted out at its core. Our ERA framework of education, regulation, and automation helps to ameliorate such problems. This can be most effectively implemented by introducing a technology diplomat across NATO member states. By educating populations of NATO member states through the technology diplomat, resilience can be enhanced through improved tech literacy. Regulation can be addressed by the tech diplomat, who will work to transcend constitutional doctrines to form a unified front against big tech. The AI needed to stunt disinformation at its birth already exists, and it will be the role of our techplomacy to ensure it is deployed unilaterally across all of our member states. The key to our ERA policy is the belief that one sharpened spear is always more effective a thousand individual needle pricks.

TEAM NAME: The Chasers

AUTHOR NAMES: Pashion Israel, Samantha White, Lauren Napier, Sumandeep Ghataora

AFFILIATIONS: Converse University, Spartanburg Community College

SUMMARY: The topic of disinformation is a pertinent issue for our world today. While we cannot eradicate this problem entirely, we can slow it down. Our team has taken the education route to help our individual populations better their knowledge and understanding of AI attacks. We believe that through education we can identify and attack the problem at its base and inform all ages on how they can personally combat this. Additionally, we believe that through developing stronger AI defence programs we can better prepare social media outlets and public/private institutions for an attack. Both the created guidelines and defence program will build both better capacity and trust amongst member states and institutions. The education program will allow the population to enhance their research skills to prevent AI attacks and the social media guidelines and AI programs will help tackle the problem head on.

TEAM NAME: NATO Your Business

AUTHOR NAMES: Jonah Sweidan, Claire Rudinsky, Mandy Mueller, Samuel Huff

AFFILIATIONS: William & Mary

SUMMARY: Bots are able to proliferate on platforms and spread disinformation easily due to a lack of authentication and a failure to effectively trace posts and narratives. Identifying patterns more efficiently will enable NATO members to respond to threats faster. Efficiency will be increased through automatic tagging algorithms, adapting those used to identify trending topics to ping specific key words that suggest a threat to national security. More extensive use of authentication software, such as reCAPTCHA, could help reduce the proliferation of bots on platforms, curbing the rate at which disinformation spreads. Public acceptance of new measures can be increased through the use of transparency campaigns that employ celebrities and non-partisan figures to legitimize proposed changes.

TEAM NAME: ODU CyberSecs

AUTHOR NAMES: Jada Cumberland, Kahlia Douglas, Elijah Gartrell, Timothy Platt, Brandon Zakaras

AFFILIATIONS: Old Dominion University

SUMMARY: We propose the implementation of special investigatory teams created by NATO to identify, investigate, and share potential social media bots. Artificial intelligence (AI) will automate the identification of potential

bot posts on social media sites through filtering methods such as key phrases and flagging. Members of the team will investigate and validate the findings. By implementing a human factor, we can distinguish between AI and human posts. Private company liaisons will then share reviewed and compiled information. This team will also encourage reporting of suspicious accounts or activities from companies to be shared with the rest of the industry.

In the future, we can prevent the spread of disinformation by educating the masses on critical thinking methods and instilling fact-checking habits by introducing these skills.

GOLF STREAM: PUBLIC HEALTH

TEAM NAME: VU/EMI

AUTHOR NAMES: Mahima Jayaraj, Elin Plette, Ilaria Sarti

AFFILIATIONS: Vrije Universiteit Amsterdam

SUMMARY: The proposed solution is to focus on how information is screened to identify misinformation, and how the knowledge and data collected from the screening process is used to devise proactive solutions for the future.

Data collection should be done in a hybrid model which contains an algorithm and crowdsourcing. Each individual country devises this mechanism in accordance with their privacy laws. NATO will act as communication channel among NATO members and set standards on formulating the screening process. The relevant screened information from member countries is then consolidated on a NATO wide level to identify general trends and vulnerabilities. This data is invaluable to NATO members for presenting a coordinated front against misinformation and coordinated misinformation attacks. NATO also creates public polls and uses algorithmic functions as a self-evaluation mechanism.

The information can also be used to create predictive mechanisms which over time help us fight coordinated misinformation better.

TEAM NAME: Team VU

AUTHOR NAMES: Moritz Tolle, Moritz Hawel, Cornelius Müller, Nikita Kirzyk, Henri Rau

AFFILIATIONS: Technische Fakultät Albert Ludwigs Universität, Vrije Universiteit Amsterdam

SUMMARY: Creating a position of health specialist who would be the head of a multinational gremium consisting of medical special and scientists from allied nations. The gremium will be in charge of fact checking and peer reviewing the scientific information from articles worldwide. The information that passes the check will be certified with a "NATO Healthcare Council Approved mark," which will then be given to the articles that pass the check to highlight their credibility (same as the Instagram checkmark). The health specialist will then gather all of the approved data and present it before the allied governments and advise the nation's' public policies based off the scientific findings. This will help nations to build their public health policies around trustworthy data. Additionally, the gremium could warn nations about impending disinformation attack and warn of certain practices. Providing the different countries with bias-free information to ensure accurate steps from government and protect society.

TEAM NAME: Neighbour Susan

AUTHOR NAMES: Annie Rose Greenman, Dylan Lampe, John Aslanes

AFFILIATIONS: Rochester Institute of Technology, James Madison University

SUMMARY: NATO Public Health Education Association (PHEA) is an organization where public health professionals and researchers can submit studies for peer review. Once reviewed by 8-12 researchers per review from 20 of the NATO countries, it will be published with the endorsement of NATO's PHEA, their goal: to educate global communities from a well-regulated, credible source. PHEA publications can be found on their verified social media accounts, their website, and through publicly funded areas (universities, libraries, health centres, etc.) Organizations such as WHO can rely on PHEA's educational publications can implement them into medical use and beyond public education. Although it will take time to build trust, PHEA can be organized and staffed in four months with a goal of the first publication in six. Overall, a global network of connections will be created and used in order to maintain good public health information and protect the citizens of NATO countries.

TEAM NAME: Truth seekers

AUTHOR NAMES: Băluță Andreea-Cristina, Borcoș Cristina-Ionela, Coroiu Florentina-Cătălina, Mîndrescu Cezara-Mihaela, Strempel Christian-Gabriel

AFFILIATIONS: Carol I National Defence University, University of Bucharest, Transilvania University of Brasov

SUMMARY: The platform's mainly purpose it's an efficient communication over the disinformation problems over NATO. It should be a place where member countries work together in order to counter disinformation and make team over fake news problem. Fake news is just a digital war. The enemy is invisible, but NATO's force, as alliance, should be visible. Social Media is the biggest fake news spreading area and the alliance should protect it in order to maintain global safety. With the purpose of that, all countries should work together to fight this enemy.

TEAM NAME: Zoot Your Zot

AUTHOR NAMES: Noel Ang Cheng Kai, Caleb Wensloff, Deng Liu, Adam Erik Xavier Hansen, Iku Nakamura

AFFILIATIONS: University of California, Irvine, Sophia University

SUMMARY: We propose that NATO works to create an effective reporting network by partnering with Civil and Commercial Organizations to rapidly identify new outbreaks of disinformation. NATO will respond to this by launching a media campaign tailored to match the sources of disinformation to quickly discredit and limit its spread. This will be followed by an educational outreach programme, to help raise awareness in the local community on how to identify and avoid falling victim to disinformation. The end goal is to build a robust reporting network which can help alert NATO and allow them to rapidly respond to disinformation while building long term resilience to such disinformation campaigns through education.

TEAM NAME: Canterbury Christ Church University

AUTHOR NAMES: Virginia Sala, Jordan Selvey, Sergio Ramiro Carretero, Jaime Valenciano Gonzalez

AFFILIATIONS: Canterbury Christ Church University

SUMMARY: Our project aimed to counter disinformation in relation to public health targeting different age groups. We recognised that since human beings change views and develops knowledge differently through the course of their lives, it is important to challenge disinformation differently in regards to children, teenagers and adults. Anti – disinformation tools for children would be included in story books and cartoons, illustrating how the main character of the story is affected by their belief in certain information. Anti – disinformation techniques for teenagers would be included at the beginning of TV series through adverts emphasising the topic of independence. In regard to adults, a big fake news that would live a fun impact on the minds of people would be implemented (e.g., Lionel Messi signing up for Wigan Wanderers) to arise awareness on how it is important to weight information. These projects would be carried out by the current NATO marketing team. proposal is orientated on the creation of a public campaign to counter combat disinformation regarding public health.

HOTEL STREAM: RUSSIA/UKRAINE WAR

TEAM NAME: The Arbiters (of Truth)

AUTHOR NAMES: Erica Buckland, Samantha Tanner, Riley Galligher

AFFILIATIONS: University of Texas at Austin

SUMMARY: NATO has vast language capabilities, yet the scale of disinformation across languages is overwhelming, resulting in gaps in NATO's overall Disinformation Defence Strategy. We propose a three-pronged approach of crowdsourced data gathering, NATO analysis and fusion, and membership engagement and action. In our high-level crowdsourcing, we will partner with technology companies, social media companies, and regional language experts to canvas non-English disinformation operations of a greater scope. This data will provide NATO with more resources to process and integrate the data into action-based briefings to better equip member states and strategy. With the coordination of language expertise and high-level analysis, member states can use the action briefs to combat disinformation with counter narratives, pre-bunking, and volunteers who aid in identifying and reporting disinformation actors. Smaller languages are most vulnerable to Russian disinformation, and without NATO's efforts to equip these nations with defences, we will lose whole nations to information disorder.

TEAM NAME: UMass Amherst

AUTHOR NAMES: William Hogan, Joshua Ruggieri, Stephen Baiardi, Benjamin Chevrette

AFFILIATIONS: University of Massachusetts Amherst

SUMMARY: Our team's proposed COA is for NATO to fund the production of a docudrama series which combines expert interviews and real footage with dramatic narrative. This documentary will use a pathos approach to counter overarching Russian disinformation campaigns where it matters most: the Russian populace.

This solution addresses several fundamental problems with NATO's counter-disinformation campaigns: they lack entertainment (and therefore engagement) value, fail to reach impactful audiences, and are reactive in nature. This docu-drama would follow a similar format to the recent Netflix docudrama The Social Dilemma which presents well researched information alongside dramatized scenes to boost entertainment value; therefore, increasing engagement with the layperson. By targeting the docudrama to the Russian populace this effort will reach audiences traditionally unexposed to NATO campaigns, allowing NATO to seize the initiative in framing narratives.

This is a feasible and scalable COA which does not violate NATO guidelines, and offensively contests Russian disinformation.

TEAM NAME: CSD Rovilo

AUTHOR NAMES: Pablo Rodriguez-Villanueva, Nathalia Lozano, Lulu Victoria

AFFILIATIONS: University of Navarra

SUMMARY: The project recognizes a lack of unity and need for re-localization within existing efforts, and thus utilizing methods that will create both empathetic and lasting emotions. In consideration of this, we have developed a set of recommendations where NATO can achieve to strengthen their foundation in member-states, as well as work with a targeted population within Russia that we know to be the most vulnerable to manipulation and lack of information. This will be done through a collaboration with existing efforts within NATO, such as the #WeareNato and Protect the Future, in order to create a more long-lasting reaction, channelling NATO efforts and giving it a wider base through which to have more impact.

TEAM NAME: Splinter Cell

AUTHOR NAMES: Nikita Mishankin, Izabelle Apostol, Sabin Rufa, Ruslan Chyrva

AFFILIATIONS: University of Warwick

SUMMARY: To counter Russian wartime disinformation, we plan to create an organisation with regional headquarters to tailor the approach on counterpropaganda to each region. The headquarters would have three departments. The first would locate and analyse the disinformation to create and distribute counterpropaganda material to the general public. The second will focus on creating and improving online automated response strategies through analysing the spread of propaganda and working with tech companies to establish cooperation between big tech and NATO. The third would focus on interactions between the organisation and volunteer groups. Our counterpropaganda will have an emphasis on rhetoric, myth, and symbolism to promote solidarity and identity within NATO countries and allies. This will be done through creating an identity for NATO of being defenders of democracy, peace, and liberty. This will be achieved through several engagement streams and approaches, by using human and technological resources.

TEAM NAME: Aston Bulls

AUTHOR NAMES: Jude King, Ashvini Jayanthan, Tolu Olagunju

AFFILIATIONS: Aston University

SUMMARY: Continuing to ally with and influence the decision-making of mainstream Western social media platforms, including Facebook, Twitter, Instagram, and TikTok, in the fight against pro-Russian disinformation and propaganda; continue to restrict the ability of bots and fake account to spread this disinformation, while bolstering the current capabilities of these platforms to fact-check and reduce falsehoods. Recommend social media platforms to work with tech companies to develop GDPR compliant AI content moderator that identify and targets bots.

Use all available Russian-speaking social media and news channels to combat Russia's 'Ukraine and the West are the aggressors' narrative; use of shocking imagery of Russia's actions in occupied Ukraine, including showing the massacres that have occurred and the deliberate shelling of civilian areas, and showing positive-Ukraine imagery, such as soldiers being greeted in liberated territories; as well as debunking Russia's one-nation narrative and historical revisionism through the use of the Russo-Ukraine agreement on

nuclear disarmament and Ukraine’s vote on independence from the Soviet Union.

Where available, use pro-Western social media accounts, such as those on Facebook, Twitter, Instagram, and TikTok, to spread factful information on the Ukraine War, including pro-Western narratives, linking to the second point about showing Russian actions.

Sleeper sites are used by Russia’s side. SEO services with facts, NATO – setting the record straight. This surpasses sleeper sites and allows users to see NATO fact-based content as the first search.

INDIA STREAM: TERRORISM

TEAM NAME: Team University of Florida

AUTHOR NAMES: Maya Razdan, Connor Panish, Tomas de la Huerta

AFFILIATIONS: University of Florida

SUMMARY: NATO will partner with small and growing social media companies to provide sentiment analysis software and implement chat-flagging systems. They will be incentivized to partner with NATO through the formation of a financial support network, creating a mutually beneficial relationship between NATO and the growing social media sector. In addition, this partnership will pressure larger companies to work with NATO and implement their own solutions. Furthermore, by partnering with smaller companies, the future sector of social media is cornered, allowing NATO to stay ahead of terrorist activity. To implement this, a task force will be formed with a Computational Linguistic Unit which improves sentiment analysis software, an Implementation Unit which runs the software, and an Outreach Unit responsible for partnering with companies. Overall, this bottom-up approach allows NATO to limit terrorist-related disinformation by disseminating flagging software and forming a strong relationship with the ever-changing social media landscape.

TEAM NAME: Blue Fire

AUTHOR NAMES: Stefana Velescu, Eula Mengullo, Alexandra Sheard

AFFILIATIONS: University of Calgary

SUMMARY: Our group came up with the idea of a NATO Strategic Council of Cybersecurity that will expand educational access to the greater public.

NATO can help the existing AI technology of different social media platforms by offering support regarding accessibility to more languages and data for nuanced and stylistic differences in propaganda. Also, it can help manage heavy data analysis demands and implement the Redirect Method by using an AI to analyse users' behaviour and direct them to specific content conducive to countering terrorist narratives and connecting vulnerable individuals with psychological support.

Once project parameters are developed and have reached a function to be implemented in the founding state, draft a resolution/treaty document to ensure that NATO member states domestic policies and legal orders are being respected. Considering the potential implications of sovereignty cost, using a treaty to guide and regulate the project will provide a clear path to long term implementation, regulation, and support of the project, especially as it grows from one member state to another.

TEAM NAME: Francisco Comillas "El Autónomo"

AUTHOR NAMES: Gonzalo Manzano Ortiz, María Gracia Moreno Vegas, María Sureda Sanchez, Marcos Checa Rubio, Clara Sanchez Portela

AFFILIATIONS: Universidad Autónoma de Madrid, Universidad Francisco de Vitoria, Universidad Pontificia de Comillas

SUMMARY: How to deactivate disinformation as a tool for extremist and terrorist radicalization and recruitment efforts? In leu of article 10 of NATO's Strategic Concept, our team proposes a three branch solution to counter the capabilities of transnational threats by: 1) redirecting the public towards safe and true information through dynamic P2P and disruptive social media campaigns, that utilize NATO's own outreach capacities to their fullest, as well as algorithmic de-radicalization through content verification and "redirection"; 2) redefining NATO's short and long term relationships with private sector key strategic firms and non-state actors, enhancing the participation of civil society in the safeguard of our shared cyberspace; and 3) establishing new focus points and tools for NATO's role as a cyberspace

guardian, through ethical/lawful hacking of potentially unsafe domains, launching birdwatch operations in new geostrategic non-NATO regions, and close cooperation with EU's projects such as CLAUDIA to boost NATO's DIANA programme.

TEAM NAME: PPEople

AUTHOR NAMES: David Gerard Nandjila Alders, Laura Buettner, Javier Santos Ripa Ramstroem, Ahmad Fikri Dweiri

AFFILIATIONS: Vrije Universiteit Amsterdam

SUMMARY: Extremist and terrorist groups use social media for communication, reaching potential recruits and planning attacks. We want to focus on disrupting the recruiting process by building the youths' digital resilience and media literacy, starting at a young age in a playful way and building up to recognise disinformation and propaganda by introducing a standardised learning platform used by schools, a rather inexpensive and effective measure. We want to implement this with the help of all the relevant stakeholders, member states, education ministries, social media platforms and civilians and parents, as they all are interested in combating terrorism. By providing incentives and campaigns, the support should be given. Through quarterly reports and a big annual report using the social media platforms statistics, we can measure the success of the proposal. Investing in the future, i.e. children, is very sustainable as well.

TEAM NAME: FIU Panthers

AUTHOR NAMES: Ariel Robledo, Denisse Castrillo, Natalie Martinez, Katherine Mesa

AFFILIATIONS: Florida International University

SUMMARY: Disinformation created by terrorist groups have been drastically increasing and posing a threat to the nation-states of NATO. The terrorist groups' use of social media to spread disinformation has influenced individuals in these states to follow the rhetoric imposed by the groups and have thus added to the violent attacks that occur. The implementation of the Terror Disinformation Response Hub (TDR) as a subcommittee of NATO's Civilian Intelligence Committee (CIC) would create a network of ambassadors from each member of NATO. TDR uses a phase structure to work with these ambassadors. Phase 1 researches vulnerable nations based on higher amounts of terrorist disinformation, phase 2 evaluates these threats and provides funding for training in these nations, and phase 3 uses data collected to review progress made with TDR and allows nations to request extra ambassadors based on need. TDR's ambassadors would use legislation in its countries to monitor and diminish the disinformation tactics used by the terrorist organizations.

TEAM NAME: UNIK

AUTHOR NAMES: Chanté Price, Evelyn Turner, Irewamide Sofela, Jil Merlijn Abt

AFFILIATIONS: Oxford University, Innsbruck Austria University

SUMMARY: Combatting Disinformation by Terrorist and Extremist Groups. We have developed an efficient, interwoven strategy that offers a proactive response to the plague that is disinformation.
Our first approach is to increase regulation:

- Reducing the financial incentives that drive the ad-marketing ecosystem by introducing penalties or fines for inappropriate advertisements.
- Creating a representative council consisting of delegates and academics
- Strengthening the role of national courts in ensuring compliance with regulation, by updating content liability laws.
- Promoting healthy commercial interaction between companies by the de-monopolisation of the social media industry.

Our second approach is prevention:

- Investing in AI initiatives
- Utilising links with EU and UN to assist Law enforcements

Our third approach is digital literacy

- Cooperating with think tanks, academics,
- Increasing social funding EU – public, free courses; information boxes mandated; adverts; campaigns in schools and the workplace
- Introducing Simple, understandable information considering language barrier issues;
- Taking a Citizen-focused approach.