EISS 2023
Open Panel Proposal

Title

Addressing Wicked Problems in Cyber Conflict

Chair

Julia Carver, University of Oxford
julia.carver@politics.ox.ac.uk
United Kingdom, ECR

Discussant

Samuel Seitz, University of Oxford & RAND Corporation
samuel.seitz@balliol.ox.ac.uk
United Kingdom - United States, ECR

Abstract

The cyber domain is filled with “wicked problems” (Churchman 1967, Rittel and Webber 1973, Conklin 2006). Be they how and when to attribute a cyber attack, how democracies should respond to election interference, integrating the cyber domain in wargames, or finding the best models and experimental methods to understand international cyber security.

Because they are the "symptom or result of multiple, contingent, and conflicting issues" (Marshall 2008), all of these questions are plagued with complexities that we are just beginning to comprehend. They require an interdisciplinary approach and the creation of a strong epistemic community. Therefore, this panel brings together scholars and practitioners of cyber conflict in the mindset of war studies approaches. We will tackle these important issues by shedding light on how human agents, organisations, and technology interact with each other in the context of cyber conflict, widely understood. Our discussant will then leverage problem structuring methods (Rosenhead 1989) to provide a common methodology to apprehend them.

In line with the spirit of the conference, we have put great emphasis on diversity and representativity, with the presence of Eastern and Southern European institutions, of experimental and epistemological approaches, as well as policy-makers and embedded scholars. Members of the panel and authors are in majority early-career researchers, and have a 50-50 gender balance.

PAPER ABSTRACTS

Paper 1
The Normative Power of the Factual: How State Practice Shapes Understandings About Direct Public Political Attribution of Cyber Operations

Authors

[Speaker] Christina RUPP, Stiftung Neue Verantwortung
crupp@stiftung-nv.de
Germany, Science & Technology Studies

Dr Alexandra PAULUS, Stiftung Neue Verantwortung
apaulus@stiftung-nv.de
Germany, Science & Technology Studies, ECR

Abstract

An increasing number of states use direct public political attribution to call out inappropriate behaviour in cyberspace attributable to another state. Shared understandings about conducting and communicating political attribution practices are essential to avoid misunderstandings and mitigate the risk of potential escalation between states. However, attribution remains only marginally addressed in the context of diplomatically negotiated cyber norms so far. This makes this policy instrument well suited to explore the formation of normative ideas through state practice as it leaves ample room for practical interpretation by states.

Based on a selection of five case studies, this paper identifies which cyber operations the selected states have publicly attributed, how the attribution was communicated and justified, to what extent other states were involved in the process, and how other states perceived the attribution. This analysis of established and emerging state practice will permit new insights into how States currently perceive the respective normative framework, that is, formalised cyber norms, and conclusions as to what extent the observed State practice gives rise to new shared understandings about appropriate state behaviour - practised cyber norms - when it comes to direct public political attribution of cyber operations.

Paper 2

A Lesser Evil: Why Democracies Struggle to Respond to Cyber-enabled Election Interference

Author & speaker

Arthur LAUDRAIN, University of Oxford
arthur.laudrain@cybersecurity.ox.ac.uk
United Kingdom, Mixed Methods Foreign Policy Analysis, ECR

Abstract

Recent episodes of foreign meddling in elections in the U.S., France, and the U.K. have led observers asking whether democracies could uphold their electoral sovereignty in the 21st Century. Free and fair elections are the cornerstone of democratic regimes, and such encroachment on a people' sovereignty and self-determination would be expected to trigger a strong response from the affected states. Yet, what we have witnessed ranges from unspecified threats and diplomatic sanctions to total inaction. How can we explain this response? In other words, why democracies fail to counterbalance against the threat of foreign interference into their electoral processes?

In a previous paper, I argued that neoclassical realism's position in the agency-structure debate makes it particularly apt at tackling cyber-enabled foreign election interference (CYFI) research problems. In this new paper, I test this theory with primary empirical evidence. Focusing on election interference episodes of 2016-2017, I conducted dozens of elite semi-structured interviews with direct participants in the foreign policy and national security policy-making process of their respective governments. I adopt a methodological synergy design. On the one hand, I probe the internal validity of the theory with a causal narrative. I combine it with an internal comparison as the primary method to generate evidence from causal process observations. On the other hand, I probe external validity with cross-case analysis in the form of a multistage Millian method, generating evidence akin to dataset observations.

I find that foreign policy response to CYFI is a consequence of a balancing by decision-makers between the structural stimuli of components of power and a combination of intervening variables relating to threat perception and public opinion constraints. I then discuss the important policy implications of these findings, highlighting the need for a whole-of-society approach to tackling foreign interference.

Paper 3

Numbers Prediction and Cyberwar: Why Integrating the Cyber Domain in Kinetic Wargames Is So Difficult and What Can Be Done

Author & speaker

Peadar Charles Callaghan, Tallinn University
peadar@tlu.ee
Estonia, Wargaming, ECR

Abstract

How do we prepare for a developing reality that has little to no historic precedent? How do we adequately prepare for cyber-enabled conflict where the 'fog of war' is exacerbated in the virtual domain, resulting in greater uncertainty? Wargames have been used throughout history to train for realities that have yet to happen; be they theoretical conventional battles or full scale nuclear conflict. For this reason the introduction of the cyber domain into kinetic or joint wargames has become an area of interest for both planners and game designers.

The integration of the two forms of warfare gaming (cyber and kinetic) into a coherent system has proven elusive and problematic. The Quantified Judgment Model (QJM) of Dupuy (1979) has gone on to inform and impact wargame design such as the Tactical Numerical Deterministic Model (TNDM) (Lawrence 2017). The QJM uses seven characteristics to generate the Operational Lethality Indices (OLI) of conventional weapons. By applying these indices to cyberweapons it becomes clear that they are fundamentally different from kinetic wargames weapons.

This paper argues that cyber weapons cannot simply be plugged into large scale kinetic wargames. It offers an overview of the methods that can be used to add the cyber domain to such games. These range from the use of umpires as proposed by Curry and Drage (2018), to the use of cyber ranges to gather realistic attack and defence data. This paper also critiques the various approaches and outlines suggested directions for future studies in order to make these games as realistic as possible.

Paper 4

Overcoming Obstacles: Reflections on Creating a Cross-National Experimental Cyber Security Research

Authors

[Speaker] Ayhan Gücüyener Evren, Kadir Has University
ayhangucuyener@khas.edu.tr
Turkey,, Methodology in Social Sciences/Decision Making, ECR

Dr. Salih Bıçakcı, Kadir Has University
asbicakci@khas.edu.tr
Turkey, Methodology in Social Sciences/Decision Making

Abstract

Because of the pervasiveness of digital technologies, academic interest in cybersecurity studies from all disciplines has surged. Cyber threats have become a compelling problem for international security and the object of a growing interest in International Relations (IR). IR scholars have sought to catch up with the empirical evolutions of conflict in cyberspace; to unpuzzle motivations behind state interactions in this domain. However, rigorous scholarship, in particular theorisation and conceptualisation (Smeets 2022, Egloff 2022) remains at an early stage. Still today, the field needs progress in methodological tools (Stevens 2018).

While the literature has been primarily focused on meta-theoretical work, one of the methodological advances in cybersecurity studies has been the application of Foreign Policy Decision Making (FPDM) methods that include scenario playing and simulating. As McDermott (2019) and Gomez (2021) pioneered the “cognitive turn” in cybersecurity studies, this approach allows looking beyond the black-box of the state, by shifting to an agent-oriented system. All the while, scenario-based experiments can provide cybersecurity scholars with a fertile ground to observe decision-making dynamics (Gomez and Whyte 2022). However these tools are not the panacea, and there are significant obstacles in developing an experimental design, primarily when research is conducted in a comparative approach.

On this basis, the purpose of this paper is to discuss the methodological framework in an ongoing comparative study that looks at decision-making dynamics of cybersecurity professionals, using a scenario-based experimental design. The study will also discuss difficulties in developing cyber threat scenarios, in a domain that differs significantly from that of the kinetic domain. This paper will also address potential deadlocks in conducting cross-national cybersecurity research, such as difficulties in matching samples, the fragility of trust between agents, and other barriers to information sharing.