Australian National University

STRATEGY AND STATECRAFT IN CYBERSPACE

Research Program Guide: February 2016

National Security College

Crawford School of Public Policy

ANU College of Asia & the Pacific

OUR PARTNERS

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

The Centre for Applied Cybersecurity Research is distinctive in interweaving technical and policy expertise. The Center draws on Indiana University's wide range of scholarly expertise in computer science, informatics, accounting and information systems, criminal justice, law, organisational behaviour, public policy, and other disciplines, as well as the extensive practical cybersecurity experience of its operational units.

RAND EUROPE

The RAND Europe Defence & Security team conducts a broad range of research for policy makers in Europe and beyond. The RAND Corporation has long been recognised for its contributions to defence and security policy. RAND Europe furthers this tradition by offering a dedicated research team with wide-ranging expertise, covering key defence issues such as equipment acquisition and personnel policy, and security issues ranging from those in the domestic arena to those that are international concerns.

MUNK SCHOOL OF GLOBAL AFFAIRS
UNIVERSITY OF TORONTO

The Munk School of Global Affairs is a professional degree-granting interdisciplinary school focused on global issues. Its mission is to deeply integrate research on global affairs with teaching and public education, and it is the home of world-renowned researchers and more than 30 academic centres and initiatives.

Charles Sturt University

The Centre for Research in Complex Systems at Charles Sturt University was formed to carry out world-class research in complex systems theory and applications in socio-economic systems, business and human cognition. The many projects have covered a range of themes, from fundamental analysis of cellular automata through to agent based modelling, virtual environments and games.

ECUSRI
Edith Cowan University
Security Research Institute
AUSTRALIA ECU EDITH COWAN UNIVERSITY

With a reputation as one of the leading cyber security and digital forensic groups in the world, the ECU Security Research Institute has emerged as one of Edith Cowan University's most vital research groups. It delivers immediate and high impact outcomes in the area of digital forensics, cyber security, critical infrastructure security and human security. Ongoing collaborations with the various Australian and international partners, as well as a range of security-related research alliances are testament to the critical importance of digital and physical security in our world.

ABOUT THE PROGRAM

Launched in 2014, this international and interdisciplinary research program responds to the need to better understand cyberspace as a new domain in which states interact with each other. Cyberspace is creating enormous opportunities, but also contains poorly-understood threats to security, especially given the increasingly complex relationships between states, transnational actors and even individuals.

Our program is creating an integrated conceptual, analytical and computational modelling framework to explore these challenges. Our models allow scholars from the humanities, the social sciences and the natural sciences to work together to create and test hypotheses about security in the cyber age.

Because cyberspace is a new domain, many of its core concepts are essentially contested. And because the structure and dynamics of cyberspace are changing rapidly, those concepts are not settling.

The modelling framework being developed through this research allows tomorrow's cyberspace to be explored with the same rigour as today's. As the program continues to develop, it will provide an environment in which policy makers can road-test new policy ideas. It will also produce a hands-on environment for advanced teaching in cybersecurity, political science, international relations and international law.

The Political Ecology of Cyberspace

Cyberspace challenges national security through the increasingly complex relationships between non- and sub-state actors and the international system as a whole.

We have leveraged concepts and methodologies from ecological science to analyse global cyber security. Ecological metaphors have often been used to describe the complex interdependence among actors in cyberspace. Abstracting both ecology and international relations by treating them each as particular classes of complex systems creates a useful intellectual mechanism for facilitating these mappings (see Case Studies).

Our political ecological approach offers a dynamic and agile understanding of the action/reaction cycle in cyberspace defence and strategy. Our central contention is that policy and strategy must be allowed to evolve, just as cyberspace evolves.

Implications for national security policy and strategy

Over time, the program will articulate a policy framework for the critical evaluation (and re-evaluation) of conventional wisdoms about cyber conflict and security. As the cyber domain is an adaptive environment, it will be important to be able to assess the impact of policy and strategy on cyberspace.

Different regulatory, persuasive and coercive interventions will have different trade-offs and costs, the quantification of which must be part of risk-based policy formation and strategic prioritisation. Our research will help us question the stability of cyberspace as an environment and test its vulnerability to internal and external drivers of change.

The program will encourage diversity in the design of a range of strategic concepts and in the selection of the agent(s) best suited to the deliver them. Multi-agent responses and coalitions will be natural rather than exceptional, and will be formed at various levels between public and private actors.

Deliverables and benefits

Through papers in the peer-reviewed literature and public commentary, this project is informing the public debate on cyberspace's threats and challenges for national security policy and strategy.

It will also continue to host workshops and conferences, such as the conference on Securing our Future in Cyberspace in February 2016, for stakeholders in the government and business sectors in Australia, Canada, the UK and the US, as well as interested members of the public. These hands-on workshops allow participants to steer the research as well as generate and explore scenarios around the evolution of cyberspace. They will explore the policy implications of different cyberspace futures, such as a balkanised internet.

The modelling framework is providing an analytical environment which can support decision makers. It will create a resource for government to test policy options and for the NSC and its partners to use in advanced teaching of postgraduate students. The environment and models will simulate current and future trends, improving the ability to identify and manage risks, interdependencies and vulnerabilities.

We believe the research outputs will assist government and industry with options for development and consequence assessments. They will also provide a rich environment within which corporations can embed their own models to explore their cyber strategies.

CASE STUDIES

The emergence of hegemons

The research problem

We are using computer modelling to understand international relations as a complex adaptive system and to better explain the dynamics of interacting nation states, particularly in cyberspace. We adhere to the school of thought that modelling brings us closer to an experimental science of history by allowing us to study a whole ensemble of 'alternate timelines'.

What we did

We created models of states competing and cooperating in an abstract network of interactions and striving to increase their wealth and power. These models were sufficiently general for the insights gained to be transferable, with some confidence, to the real world.

What we found

Although all states in the model begin life equal in power, a single hegemon (with disproportionate power) emerges under a wide range of conditions. But a hegemon, once it emerges, does not last forever (see Figure 1), and in a domain of diffused power, like cyberspace, hegemons have more difficulty maintaining their status.

So what?

This is a comforting result. The existence of hegemons looms large in international relations theory, and underpins a raft of assumptions about states from the Pax Romana through the British Empire to the American Century. But the modelling shows that hegemony is a property of the system, not of a state. Hegemons are a part of the same dynamics as the other states (see Figure 2) – they are just the ones that end up at the top. Each individual hegemon became one through a specific series of events, but if it had not, another would have taken its place. The specifics are 'history' but the general pattern is a law of nature.

This view is not apparent from historical study alone, because the observable cases are too few. Hegemons can look exceptional, even pre-ordained. Modelling is needed to reveal the true relationships and dynamics – and hence allow new possibilities for strategy.

This study is being prepared for publication in the Journal of Artificial Societies and Social Simulation.

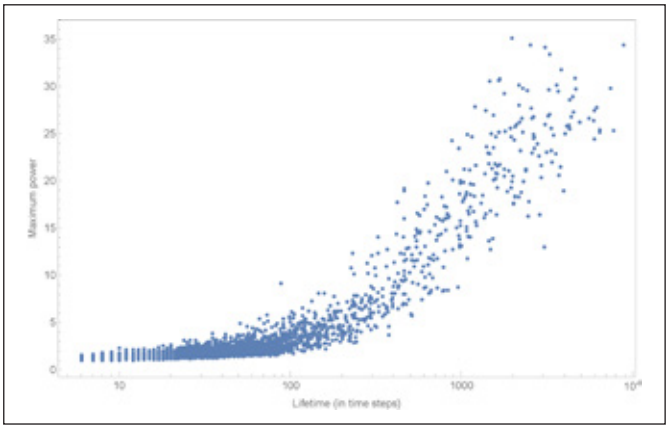


Figure 1 shows the power of a set of 20 countries (in different colours) cooperating and competing over time in a typical model run. We show, for illustration, time steps from 1000 to 2000. Most of the countries are hard to see as they have very low power. The longevity, collapse and replacement of hegemons can be seen clearly.

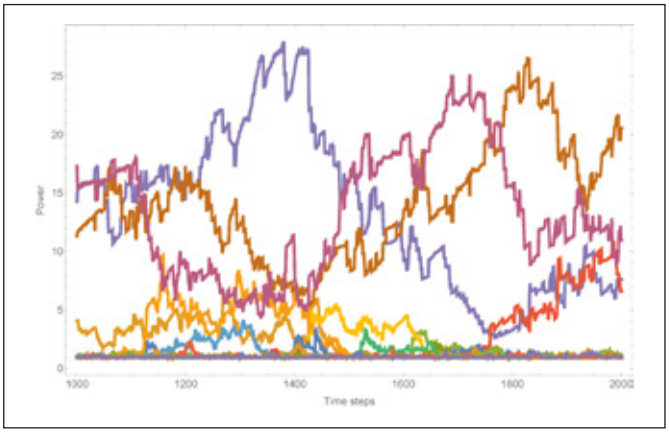


Figure 2 shows the curve (compiled over many model runs) for maximum power achieved by states versus how long they're able to hold it. All states, even hegemons, sit on the curve and are part of the same system. (Time is on a logarithmic scale for clarity).

Balkanisation of the internet

The research problem

One of the most complex, divisive and contested issues in international relations today is the governance of the internet. Broadly, the liberal democracies seek a light governance touch to best allow the free and open interchange of information across a unitary internet. Other states, particularly authoritarian ones like China and Russia, seek a much more highly regulated and government-controlled internet. In this approach, the single global internet is fragmented into a series of territorial internets each controlled by a state and connected to other territorial internets through a relatively few state-controlled channels.

This fragmentation, or balkanisation, poses a threat to the evolution of cyberspace as the key global commons of the 21st century and so poses a serious strategic threat to the liberal democracies. Keeping the internet open and free has become one of the key foreign policy objectives of the West. But balkanisation is a complex whole-of-system process. Balkanisation, at a network level, consists of changing the topology of cyberspace and could generate critical processes and tipping points.

What we did

We built some minimally realistic models — toy models — to gain some understanding of the potential for balkanisation ideas to spread across the internet and to model strategies to counter such behaviour. We investigated the potential to pass tipping points when balkanisation easily spreads.

What we found

In our experiments with simple (but plausible) growing internet-like networks, we modelled the behaviour of two sorts of nodes — 'countries' and 'other'. When country nodes have simple strategies to neutralise perceived threats arriving through the network, other nodes quickly relink to country nodes at the expense of linking to other nodes (see Figure 1). This rapidly and terminally balkanises the network (see Figure 3). Once it comes into existence, the balkanised network then acts as a strong attractor during further growth of the network.

So what?

These results suggest that, under simple but plausible rules, balkanisation is surprisingly easy to achieve and surprisingly difficult to undo. Preventing its emergence will require the West to develop new and more subtle strategies.

This study is being prepared for publication in the Journal of Cybersecurity.

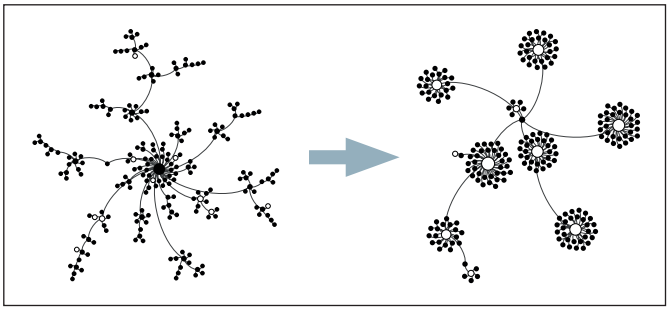


Figure 3. A simple model network of 10 country nodes and 200 other nodes first forms a scale-free internet-like network after growing by 'preferential attachment' (left hand side). Then, after about 15,000 more iterations, the network evolves to a stable balkanised network (right hand side) as country nodes filter threats that pass across the network. [Open circles = country nodes, solid circles = other nodes; circle diameter proportional to number of attached nodes.]

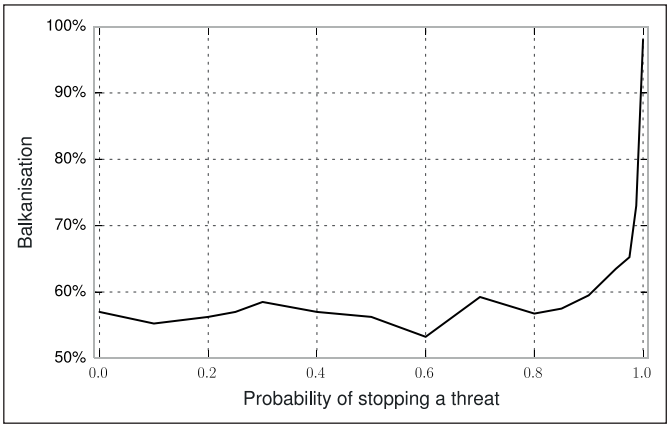


Figure 4. The change in the level of balkanisation of a simple model network (see Figure 3 above for description) as country nodes progressively increase their ability to filter threats. The network reaches a tipping point and completely balkanises once the filtering ability reaches a threshold level.

THE NATIONAL SECURITY COLLEGE

The National Security College (NSC) is Australia's leading provider of national security teaching, research and outreach.

A joint initiative of the Australian Government and The Australian National University, we build strategic understanding and critical thinking about national security. As a specialist graduate school and executive education provider at the ANU, we are shaping a new generation of leading national security professionals for Australia, our region and the world. Cyber security is a core area of the NSC's research expertise. Combined with other theme areas assessing contemporary geopolitical trends, transnational threats and future 'over the horizon' challenges, the NSC is a hub for informed analysis and cutting-edge scholarship on issues of critical importance for Australia and its partners.

Policy engagement and executive development

The NSC's research experience informs our academic, short course and policy engagement programs. For example, the NSC was engaged by the Department of the Prime Minister and Cabinet to undertake industry and academic consultations to inform the government's Cyber Security Review. We designed and facilitated two workshops culminating in a series of policy recommendations provided to government which addressed: policy; architecture; information sharing; legislation; education; and innovation.

The NSC offers Statecraft and national security in cyber space as a graduate studies course, a Cyber Challenges for National Security Agencies and Departments professional development short course and material relating to cyber security in all executive development programs. Other selected professional short courses incorporate cyber security content as appropriate.

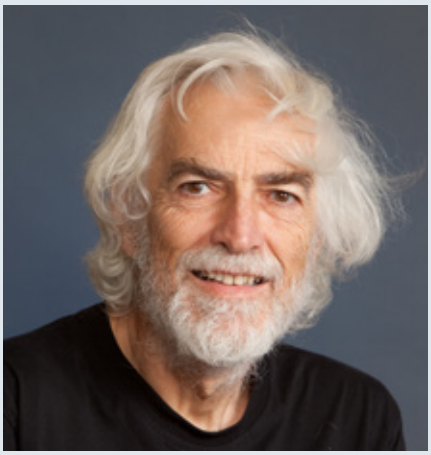
PRINCIPAL INVESTIGATORS

Professor Roger Bradbury
is a complex systems scientist with experience in international cyber issues and is with the National Security College at ANU

Professor Fred Cate
specialises in information privacy and security law issues, and is Vice President for Research at Indiana University, USA

Professor Paul Cornish
is an expert in cyber security and cyber war, and is Research Group Director for Defence, Security and Infrastructure at RAND Europe, UK

Dr Jon Lindsay
is a political scientist with research interests in the impact of technology on global security at the Munk School of Global Affairs, University of Toronto, Canada



Professor Terry Bossomaier
is a computational scientist with interests in the theory and applications of complex systems and is Strategic Professor in Computing and Information Technology at Charles Sturt University

Adjunct Professor Gary Blair
has more than twenty-five years' experience in IT within the banking, finance and other technologically intensive industries, and is with the Security Research Institute, Edith Cowan University.

CONTACT US

National Security College
Crawford Building #132
1 Lennox Crossing
The Australian National University
Canberra ACT 2601, Australia
T +61 2 6125 1219
E national.security.college@anu.edu.au
W nsc.anu.edu.au
@NSC_ANU
National Security College

CRICOS Provider #00120C

MO_NSC16036