VOLUME 19 ISSUE 2 2013 ISSN: 1192-6422

Canadian Foreign Policy Journal

La politique étrangère du Canada

From Cybercrime to Cyberwar: Meeting the Security Challenges of the 21st Century

CFPJ

Routledge
Taylor & Francis Group

Aim and Scope: *Canadian Foreign Policy Journal* (*CFPJ*) is a fully peer-reviewed interdisciplinary journal published three times a year by the Norman Paterson School of International Affairs (NPSIA) at Carleton University, in Ottawa, Canada. Established in 1992, CFPJ is now Canada's leading journal of international affairs. The Journal's international advisory and editorial boards reflect diverse political, disciplinary, and professional perspectives. Contributors are drawn from Canada and around the world. Essays are fully referenced, peer-reviewed, authoritative yet written for the specialist and non-specialist alike. Our readers include government officials, academics, students of international affairs, journalists, NGOs, and the private sector. *Canadian Foreign Policy Journal* is indexed in the Canadian Business and Current Affairs Index and the Periodicals Index.

Editorial correspondence should be addressed to: Canadian Foreign Policy Journal/La politique étrangère du Canada, Carleton University, 2116 DT, 1125 Colonel By Drive, Ottawa, ON, Canada, K1S 5B6.
Email: cfpj@carleton.ca

Business correspondence, including orders and remittances relating to subscriptions, back numbers, and sample copies, should be addressed to: Routledge Journals, Taylor and Francis Customer Service, Informa UK Ltd, Sheepen Place, Colchester, Essex CO3 3LP, UK. Email: subscriptions@tandf.co.uk

Typeset by Techset Composition India (P) Ltd, Chennai, India.

Printed and bound by Yurchak Printing Inc., USA

SUBSCRIPTION INFORMATION

Canadian Foreign Policy Journal, Print ISSN 1192-6422, Online ISSN 2157-0817, Volume 19, 2013

Canadian Foreign Policy Journal (www.tandfonline.com/rcfp) is a peer-reviewed journal published in March, June and September by Taylor & Francis, 4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN, UK.

Institutional Subscription Rate (print and online): $383/£231/€306
Institutional Subscription Rate (online-only): $335/£202/€268 (+ VAT where applicable)
Personal Subscription Rate (print-only): $68/£40/€53

Taylor & Francis has a flexible approach to subscriptions, enabling us to match individual libraries' requirements. This journal is available via a traditional institutional subscription (either print with online access, or online only at a discount) or as part of the Economics, Finance, Business & Industry Library. For more information on our sales packages please visit http://www.tandfonline.com/page/librarians.

All current institutional subscriptions include online access for any number of concurrent users across a local area network to the currently available backfile and articles posted online ahead of publication.

Subscriptions purchased at the personal rate are strictly for personal, non-commercial use only. The reselling of personal subscriptions is prohibited. Personal subscriptions must be purchased with a personal cheque or credit card. Proof of personal status may be requested.

Back issues: Taylor & Francis retains a three year back issue stock of journals. Older volumes are held by our official stockists to whom all orders and enquiries should be addressed: Periodicals Service Company, 11 Main Street, Germantown, NY 12526, USA. Tel: + 1 518 537 4700; fax: + 1 518 537 5899; email: psc@periodicals.com.

Ordering information: Please contact your local Customer Service Department to take out a subscription to the Journal: **USA, Canada:** Taylor & Francis, Inc., 325 Chestnut Street, 8th Floor, Philadelphia, PA 19106, USA. Tel: + 1 800 354 1420; Fax: + 1 215 625 2940. **UK/Europe/Rest of World:** T&F Customer Services, Informa UK Ltd, Sheepen Place, Colchester, Essex, CO3 3LP, United Kingdom. Tel: + 44 (0) 20 7017 5544; Fax: + 44 (0) 20 7017 5198; Email: subscriptions@tandf.co.uk.

Dollar rates apply to all subscribers outside Europe. Euro rates apply to all subscribers in Europe, except the UK and the Republic of Ireland where the pound sterling rate applies. If you are unsure which rate applies to you please contact Customer Services in the UK. All subscriptions are payable in advance and all rates include postage. Journals are sent by air to the USA, Canada, Mexico, India, Japan and Australasia. Subscriptions are entered on an annual basis, i.e. January to December. Payment may be made by sterling cheque, dollar cheque, euro cheque, international money order, National Giro or credit cards (Amex, Visa and Mastercard).

Canadian Foreign Policy Journal (www.tandfonline.com/rcfp) is a peer-reviewed journal published in March, June and September by Taylor & Francis, 4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN, UK.

The US annual subscription price is [$825 USD]. Airfreight and mailing in the USA by agent named Air Business Ltd, c/o Worldnet Shipping Inc., 156-15, 146th Avenue, 2nd Floor, Jamaica, NY 11434, USA. Periodicals postage paid at Jamaica NY 11431.

US Postmaster: Send address changes to Canadian Foreign Policy Journal, Air Business Ltd, c/o Worldnet Shipping Inc., 156-15, 146th Avenue, 2nd Floor, Jamaica, NY 11434, USA. Subscription records are maintained at Taylor & Francis Group, 4 Park Square, Milton Park, Abingdon, OX14 4RN, United Kingdom.

For more information on Taylor & Francis' journal publishing program, please visit our website: www.tandfonline.com.

Canadian Foreign Policy Journal, 2013
Vol. 19, No. 2, iii–vii, http://dx.doi.org/10.1080/11926422.2013.809261

Routledge
Taylor & Francis Group

Abstracts/Résumés

From cybercrime to cyberwar: The international policy shift and its implications for Canada

Avner Levin and Paul Goodrick

Countries are creating strategies to defend themselves from cyberwar and cyberespionage in response to cyber attacks such as Stuxnet, Flame and the use of social media in national conflicts. Nations are grouping in blocs for these strategies along traditional international-relations lines. Combating cybercrime is becoming more difficult, and less important, as a result, since potential partners in crime-fighting must increasingly treat each other as cyber opponents. Canada should not abandon potential partnerships with China, Russia and their allies because of increased cyberwarfare concerns. Canada should strive for a middle ground that that will allow Canada to cooperate with every country as long as that cooperation advances the Canadian interest in a more secure cyberspace for Canadians.

Du cyber-crime à la cyber-guerre: les changements de la politique internationale et leurs implications pour le Canada

Les pays inventent des stratégies pour se protéger de la cyber-guerre et du cyber-espionnage en riposte aux cyber-attaques tels que Stuxnet, Flame et le recours aux réseaux sociaux dans les conflits nationaux. Afin de mettre en place ces stratégies, les nations se regroupent, formant des blocs qui reproduisent les tendances traditionnelles des relations internationales. La lutte contre le cyber-crime devient à la fois plus difficile et moins importante, les partenaires potentiels impliqués étant de plus en plus occupés à se considérer les uns les autres comme des cyber-opposants. Le Canada ne devrait pas négliger les partenariats potentiels avec la Chine, la Russie et leurs alliés, en raison de préoccupations croissantes concernant la cyber-guerre. Le Canada devrait veiller à trouver un terrain d'entente pour pouvoir coopérer avec chaque pays dès l'instant où cette coopération fera progresser les intérêts canadiens dans un cyberespace plus sûr pour les Canadiens.

La stratégie du Canada en matière de cyber-sécurité: de la parole aux actes

Hugo Loiseau, Charles-Antoine Millette et Lina Lemay

Cet article propose une analyse du comportement du Canada dans le cyberespace et plus spécifiquement de la stratégie canadienne de cyber-sécurité. Dans cet objectif, nous tentons de répondre à la question suivante: que fait le Canada dans le cyberespace? Après avoir défini le débat théorique sur la possibilité pour les États de réguler le cyberespace, l'article décrit les étapes principales du développement de la stratégie canadienne de cyber-sécurité. Aussi, il coïncide avec le développement de la technologie informatique au début des années 90, et est accéléré dans la décennie 2001-2011 en raison d'un contexte international incertain. En guise de conclusion, l'article offre une analyse des initiatives canadiennes récentes sur la cyber-sécurité.

The Canadian cybersecurity strategy: from words to actions

This article offers an analysis of the behaviour of Canada in cyberspace, and more specifically the Canadian strategy for cyber security. To do this, we try to answer the following question : what is Canada doing in cyberspace? After defining the theoretical debate concerning the possibility for states to regulate cyberspace, the article describes the main stages of the development of the Canadian strategy for cyber security. Thus, it coincides with the development of computer technology in the early 1990s, and is accelerated during the decade 2001-2011 due to an uncertain international context. The article concludes on the analysis of recent Canadian initiatives on cyber security.

The 'wicked problem' of cyber security policy: Analysis of United States and Canadian policy response

Eloise F. Malone and Michael J. Malone

This article analyses policy response to cyber security issues. By comparing U.S. and Canadian responses, the authors conclude that the nature of cyberspace, defined as a public good with market value as well as an offensive and defensive tool, does not correspond with prevailing public policy models. The authors arrive at this conclusion by a chronological review of technological development, an analysis of conventional models, and consideration of existing public policy.

Le «caractère inique » de la politique de cyber-sécurité: une analyse des réponses politiques aux États-Unis et au Canada

Cet article analyse la réponse politique aux problèmes de cyber-sécurité. Après une comparaison entre les réponses américaines et les réponses canadiennes, ses auteurs concluent que la nature du cyberespace – défini en tant que bien public ayant une valeur marchande, ainsi qu'outil offensif et défensif – ne correspond pas aux modèles prédominants des politiques publiques. Les auteurs arrivent à cette conclusion après une revue chronologique des développements technologiques, une analyse des modèles conventionnels et la prise en compte des politiques publiques existantes.

Cyber threats and multiplier effects: Canada at risk

Angela Gendron

The defining feature of a modern, interconnected and knowledge-based society and its economy is dependence on information and communications technologies (ICT). The digital infrastructure which connects Canada's ten critical national infrastructure (CNI) sectors delivers efficiencies and opportunities – but it also comes at the cost of increased vulnerability. How to exploit the benefits and opportunities which cyberspace offers, while managing the associated risks, is an issue which is currently giving the governments of developed, cyber-dependent and globally interconnected countries considerable concern.

The low cost and anonymous nature of cyberspace makes it particularly attractive to various malicious actors; cyber criminals as well as those with political and ideological motivations, are using similar technologies and tradecraft such that the boundaries between cybercrime, cyber

espionage and cyberwarfare are blurring. States and state-sponsored cyber criminals are perpetrating high profile cyberespionage and sabotage attacks against the critical infrastructure of other states to the point where a new form of conflict seems to be emerging. There is a general consensus among developed countries that confronting these national and economic security threats requires a new approach: A response that balances a passive and reactive defense, with one which is positively aggressive and pro-active. Activities which aim at the earlier detection and identification of threat actors in order to prevent cyber attacks, as well as generating investigative leads to pursue and prosecute cyber offenders, calls for the deployment of Canada's intelligence capabilities.

Cyber menaces et effets multiplicateurs: le Canada en danger

Les caractéristiques d'une société moderne, interconnectée et fondée sur la connaissance, et de son économie, sont leur dépendance vis-à-vis des technologies de l'information et de la communication (TIC). L'infrastructure informatique qui connecte les dix secteurs d'informatique critique nationale du Canada assure des gains d'efficacité et des opportunités – au prix toutefois d'une vulnérabilité croissante. Comment exploiter les avantages et les opportunités offerts par le cyberespace tout en gérant les risques associés, est une question qui aujourd'hui préoccupe beaucoup les gouvernements des pays développés, cyberdépendants et globalement interconnectés. Le faible coût et la nature anonyme du cyberespace le rendent particulièrement attractif aux yeux de différents acteurs malveillants: de même que les cybercriminels, ceux qui ont des motivations politiques et idéologiques utilisent des technologies et des méthodes d'espionnage similaires au point que les frontières entre le cyber-crime, le cyber-espionnage et la cyber-guerre finissent par se confondre.

Les États et les cybercriminels que soutiennent les États perpétuent le cyber-espionnage et le sabotage de haut niveau contre les infrastructures critiques des autres États, au point qu'une nouvelle forme de conflit semble sur le point d'émerger. Dans les pays développés, il existe un consensus général selon lequel faire face à ces menaces pour la sécurité nationale et économique exige une nouvelle approche: une riposte équilibrée entre une défense passive et réactive, et une défense progressivement agressive et proactive. Les activités qui ont pour but la détection et l'identification précoces d'acteurs menaçants, afin de prévenir les cyber-attaques et générer des pistes d'enquêtes pour poursuivre et juger les cyber-délinquants, exigent le déploiement des capacités de renseignement du Canada.

Fallout in the Sahel: The geographic spread of conflict from Libya to Mali?

Scott Shaw

This article seeks to examine the commonly-assumed notion that the Libyan Civil War generated the current conflict in Mali. It seeks to apply the causal mechanisms from the theories of escalation and diffusion/contagion to the Libya-Mali case, to determine if such a link can be made. Using Lake and Rothchild's (1996) framework, this article finds that, with some modifications to include non-state actors, mechanisms from both theories were at play in this case. Conflict in Mali did occur as the result of escalation and diffusion/contagion mechanisms from the Libyan Civil War. The article then proceeds to outline how these mechanisms could be applied to determine if conflict could spread outwards from Mali.

Répercussions dans le Sahel: la propagation géographique du conflit de la Libye au Mali?

Cet article examine la notion couramment acceptée selon laquelle la guerre civile en Libye est à l'origine du conflit actuel au Mali. Il cherche à appliquer les mécanismes de causalité définis par les théories de l'escalade et de la diffusion/contagion au cas Libye/Mali, afin de déterminer si un tel lien peut être établi. En se basant sur le modèle de Lake et Rotchild (1996), l'article révèle que les mécanismes relevant de ces deux théories ont été en jeu dans ce cas, avec quelques modifications incluant des acteurs non-dépendants des États. Le conflit du Mali s'est bien produit conséquemment aux mécanismes d'escalade et de diffusion/contagion depuis la guerre civile libyenne.

Ensuite l'article indique comment ces mécanismes pourraient être utilisés pour déterminer si le conflit peut s'étendre au-delà des frontières du Mali.

Integrating civilian-military operations: the Comprehensive Approach and the ATF experience, 2008-2009

Nicholas Gammer

Governments everywhere are exploring the Comprehensive Approach (CA) as a more effective method of responding to security-humanitarian challenges. Most Canadian studies of the CA have focused on the military civilian tensions and inter-departmental rivalries inherent in integration. This study focuses instead on the effect of the CA on political-bureaucratic relationships as demonstrated by Canada's Afghanistan Task Force (ATF).

The ATF circumvented traditional lines of authority to become the primary institutional mainspring driving the government's foreign policy on Afghanistan. By accepting responsibility for the ATF, the Privy Council Office exceeded its traditional parameters and accepted operational responsibility. This article explores the benefits and dangers of the CA and concludes by highlighting some important issues related to the flexibility of our political system in adapting to future stabilization missions.

Intégrer les opérations civiles-militaires: l'approche intégrée et l'expérience du Groupe de travail sur l'Afghanistan, 2008-2009

Partout dans le monde, les gouvernements explorent l'approche intégrée, considérée comme la méthode la plus efficace pour relever les défis sécuritaires et humanitaires. La plupart des études canadiennes sur cette approche ont porté sur les tensions civiles-militaires et sur les rivalités interministérielles inhérentes à l'intégration.

Cette étude se focalise plutôt sur les effets de l'approche intégrée sur les relations entre politique et bureaucratie, comme en témoigne le Groupe de travail canadien sur l'Afghanistan. Ce groupe a contourné les lignes d'autorité traditionnelles pour devenir le principal ressort institutionnel conduisant la politique étrangère du gouvernement canadien en Afghanistan. En acceptant de diriger le Groupe de travail sur l'Afghanistan, le Bureau du Conseil privé a dépassé ses paramètres traditionnels et accepté la responsabilité opérationnelle du Groupe. Cette étude explore les avantages et les dangers de l'approche intégrée et, en guise de conclusion, met en avant certaines questions importantes ayant trait à la flexibilité de notre système politique en ce qui concerne l'adaptation à de futures missions de stabilisation.

Resilience or relief: framing Canada's responses to global disasters in an era of climate change

Rosalind Warner

As disasters are poised to increase in scope and frequency, it is appropriate and timely to examine the Canadian government's approach to the humanitarian challenge of global disasters through the lens of Canada's commitments to global disaster risk reduction. This article will argue, in accordance with the broad principles of disaster risk reduction (DRR) elaborated through the UNISDR process, that Canada's disaster response should pay greater attention to the need for resilience. Resilience-oriented assistance is tasked with helping communities to reduce vulnerabilities and risk by preparing for future disasters. Although it is not incompatible with relief, an orientation of resilience does contrast with one of relief in terms of the allocation of resources, the involvement of local authorities, and the underlying purpose of disaster response. Canada's recent response to the 2010 earthquake in Haiti is used to analyse the way in which disasters are framed in Canadian foreign policy, the way in which competing frames affect the provision of disaster assistance, and the effects of this framing on the recipients of disaster assistance.

Résilience ou aide d'urgence: la réponse du Canada aux catastrophes dans le monde dans une époque de changements climatiques

Alors que les catastrophes tendent à augmenter en intensité et en fréquence, il est approprié et opportun d'examiner l'approche utilisée par le gouvernement du Canada face au défi humanitaire que représentent ces désastres, à travers le prisme de ses engagements visant à une réduction des risques de catastrophes. En accord avec les grands principes définis au sein de la Stratégie Internationale de Prévention des Catastrophes (SIPC), cet article avance que la réponse du Canada aux catastrophes doit mieux prendre en compte la nécessité de la résilience.

L'aide humanitaire orientée sur la résilience a pour but d'aider les communautés à réduire leur vulnérabilité et les risques auxquels elles sont exposées en se préparant à faire face à de futurs désastres; et il est vrai que bien qu'elle ne soit pas incompatible avec l'aide humanitaire, elle diverge de l'aide orientée sur les secours d'urgence, en termes d'allocation des ressources, d'implication des autorités locales et d'objectifs sous-jacents à la réponse aux catastrophes. La récente réponse du Canada au séisme de 2010 à Haïti est utilisée pour examiner comment la politique étrangère canadienne appréhende les catastrophes, comment la concurrence entre diverses approches affecte la délivrance de l'aide humanitaire et les effets de ces «encadrements» sur les personnes à qui celle-ci est destinée.

CANADIAN FOREIGN POLICY JOURNAL
LA POLITIQUE ÉTRANGÈRE DU CANADA
Volume 19 Number 2 June 2013

From Cybercrime to Cyberwar: Meeting the Security Challenges of the 21st Century

Contents

Canadian Foreign Policy Journal, 2013
Vol. 19, No. 2, 119–122, http://dx.doi.org/10.1080/11926422.2013.805154

Routledge
Taylor & Francis Group

From cybercrime to cyberwar: security through obscurity or security through absurdity?

Alana Maurushat*

Cyberspace Law and Policy Centre, The University of New South Wales, Sydney, Australia

Keywords: cybersecurity; international law; policy

In the late 1980s, Australian hackers penetrated the United States National Aeronautics and Space Administration (NASA) computer system releasing a worm known as WANK (Worms Against Nuclear Killers). The worm was written and released as a form of protest for the NASA launch of the rocket Galileo that was to navigate itself to Jupiter using nuclear energy. The code looked threatening, with inserted expressions claiming the system would wipe all data on the network, but in fact these were merely words used in an act of political protest. The worm itself did not damage any information or research on the NASA network.

The infamous German hacker group "Chaos Club" was also busy in the late 1980s, attacking German government systems to protest against collecting and storing of census information; the groups believed that the government should not collect or store the personal information of its citizens.

Cyber attacks were launched in 2007 and 2008 against Estonia and Georgia. In the example of Estonia, the DDoS attacks crippled the government's online infrastructure, affected banking systems and had an enormous impact on the Estonian economy for years to come. In Georgia, the cyber attacks crippled the nation's infrastructure the night before Russian troops invaded. The attacks were done in such a way so that media could not report on what was occurring until after several days, as all telecommunication infrastructure was affected including the internet (to give an idea of the technical feat involved here, the internet was not affected after the 9/11 incidents).

In 2010, the Stuxnet worm made history as it spread through scada systems and, eventually, the scada control system used in the Bushehr Iranian nuclear power plant. The worm is alleged not only to have infected the control system at the plant, but also to have caused significant impairment to all research data connected to the full implementation of nuclear energy and nuclear warheads. There has been much speculation and many conflicting viewpoints on the Stuxnet worm that infected the Iranian Bushehr nuclear power plant. The principal point of contention is the identification of who wrote and distributed the worm, with speculation pointed at the United States and Israeli

*Alana has keynoted and presented at many conferences including CSI, AusCERT, High Tech Crime Conference and ISOI, and is in the media on a regular basis. She has lectured in the fields of law, criminology and computer science in Hong Kong, Canada, the United States, France, the United Kingdom and Australia. She researches and writes in the areas of cyber-security and media law with a recent book, Disclosure of Security Vulnerabilities. Alana has done consultancy work on cybersecurity, technology and civil liberties for both the Australian and Canadian governments, and for the NGO, Freedom House. Email: a.maurushat@unsw.edu.au

governments. There is no known conclusive proof that these governments were responsible.[1] There is equal speculation as to whether the worm was able to penetrate the computer systems of the nuclear power plant and, if so, whether any data was lost or altered.[2] There is, however, consensus on how the Stuxnet worm propagates. According to security expert B. Schneier:

> Stuxnet is an Internet worm that infects Windows computers. It primarily spreads via USB sticks, which allows it to get into computers and networks not normally connected to the Internet. Once inside a network, it uses a variety of mechanisms to propagate to other machines within that network and gain privilege once it has infected those machines. These mechanisms include both known and patched vulnerabilities, and four "zero-day exploits": vulnerabilities that were unknown and unpatched when the worm was released. (All the infection vulnerabilities have since been patched.)
>
> Stuxnet doesn't actually do anything on those infected Windows computers, because they're not the real target. What Stuxnet looks for is a particular model of Programmable Logic Controller (PLC) made by Siemens (the press often refers to these as SCADA systems, which is technically incorrect). These are small embedded industrial control systems that run all sorts of automated processes: on factory floors, in chemical plants, in oil refineries, at pipelines – and, yes, in nuclear power plants. These PLCs are often controlled by computers, and Stuxnet looks for Siemens SIMATIC WinCC/Step 7 controller software.[3]

Essentially, Stuxnet first propagated through a USB stick but once on the computer's systems, Stuxnet looks for PLC on Seimens' SCADA control systems. At this point, the infected machine would receive instructions from a bot and join the Stuxnet botnet.[4] The Stuxnet botnet receives instructions in a P2P channel, and operates similarly to Mebroot with the worm hiding in the rootkit. While there remains speculation as to who wrote Stuxnet and for what purpose, there seems to be consensus that Stuxnet is one of the first exceptional tools for waging cyberwar due to its ability to penetrate the control systems of critical infrastructure systems such as nuclear plants and electrical grids.

In August 2012, Saudi Arabia's national energy company, Saudi Aramco, had 30,000 of its computers infected by a worm. The anti-oppression group calling itself the "Cutting Sword of Justice" claimed responsibility for the attacks in response to the Saudi government's support of foreign regimes, such as those in Syria and Egypt, and commission of "crimes and atrocities".[5]

Cyber-security reports around the globe have alleged high-scale state-sponsored espionage of government and corporate information, most noticeably from cyber-espionage originating from China. This modern information theft (often of intellectual property) has escalated in the last decade to the point where information espionage has become the modern-day plague for governments, organizations and corporations. Information is a critical corporate assert that has become vulnerable to attacks from viruses, hackers, criminals and human error. Consequently, organizations have slowly begun the process of better securing their computer systems. Information security has never been as important as it is today for business and individuals.

Each of the above incidents is illustrative of the evolution of cyber intrusions over the past 30 years.

The terms cybercrime, cybersecurity and cyberwar are sometimes described as an evolution and, more often than not, the terms are used loosely and interchangeably.

Cybercrime is a term used to describe traditional crimes that are committed or enhanced with the use of technology, as well as new crimes that have emerged as a result of a technology such as the internet.

Cybercrime covers four general areas that are protected areas of law under the international *Convention on Cybercrime* and by most domestic law frameworks in the Asia-Pacific region. These four general areas are:

(1) Fraud and forgery
(2) Child sexual abuse materials (child pornography)

(3) Copyright infringement (intellectual property)
(4) Computer offences (involves a form of hacking) / unauthorized access and use of data, data systems and computers

Cybersecurity and cyberwar overlap with cybercrime as it is concerned with the last cybercrime category of computer offences/hacking.

Cybersecurity is the protection of data, data systems and computers from unauthorized access, modification, impairment or interference. Cybersecurity is a difficult and complex field. The political, economic, technical and legal questions surrounding it are complicated. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others.

Cyberwarfare involves actions taken to affect an adversary's information and information systems while defending one's own information, information systems and critical infrastructure. Cyberwarfare differs from cybersecurity in that the cyber-attacks are initiated through government infrastructure or are state-sponsored. The cyber-attacks must be used either in armed conflict or where there have been acts of use of force, or in the lead-up to armed conflict and use of force.

Governments around the world are engaged in developing cybersecurity strategies. In 2010, the United Kingdom released its *National security strategy*; then in 2011, *The UK cyber security strategy: protecting and promoting the UK in a digitized world.* In 2011, the United States Department of Defense launched its *Strategy for operating in cyberspace.* Likewise in 2010, Canada released its *Canada's cyber security strategy.* Russia also published views on cybersecurity and cyberwar in *Conceptual views regarding the activities of the armed forces of the Russian Federation in Information space.* In January 2013, Australia released its new national security strategy document, titled *Strong and secure: a strategy for Australian national security.* In February 2013, the European Union released its new cybersecurity strategy, *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace.* Just seven days later, the United States' Obama administration released the 2013 *Cybersecurity Executive Order.* These strategies commit billions of dollars to help fight against cybersecurity attacks aimed at businesses (e.g., intellectual property theft), banks (e.g., fraud and identity theft), and governments (e.g., defense documents). And in April 2013, the *Tallinn manual on the international law applicable to cyber warfare* was released which identifies applicable international law to times of cyber warfare. The manual provides 95 black-letter rules governing cyberwar. For instance, the manual specifically details when one may retaliate in the form of use of force or armed conflict in response to a cyber-attack. The manual

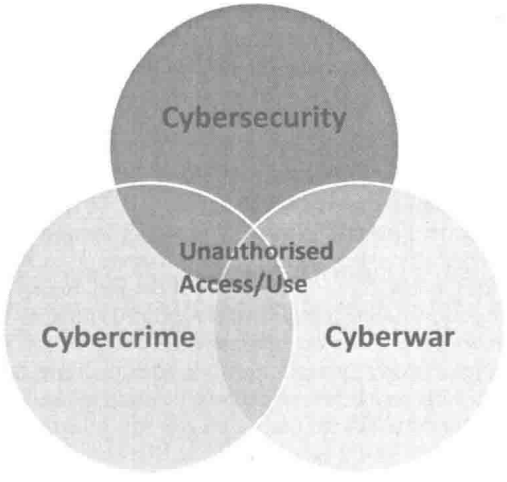

Figure 1.

goes so far as to justify the killing of hackers in times of armed conflict. Curiously, while thousands of pages are written and published on cybersecurity and cyberwar, there is little to nothing published comparatively on how cyber diplomacy or cyber peace might proceed.

Do cyber-attacks justify use of force and armed conflict responses? Does the level of obfuscation technologies make trace-back to the true source of an attack sufficiently doubtful so as to caution against any type of international sanction or use of force? How should governments engage with other countries that are known and identified sponsors of cyberattacks against their nation and businesses within their nation? Should China and Russia be singled out for the abundance of evidence that they are significant sources of cyberattacks? If so, what is the appropriate response? How should software businesses conduct their affairs with foreign entities knowing that their trade secrets are at risk? Are billions of dollars necessary to protect again cybersecurity threats? Should cybersecurity threats continue to include acts of online civil disobedience such as the overly zealous prosecution of Bradley Manning and online civil activist Aaron Schwartz? Should emphasis and money be placed on cyber diplomacy? Or has security through obscurity been replaced by security of absurdity?

This special edition of the *Canadian Foreign Policy Journal* will address many of these important issues through a Canadian lens. The problems are challenging but the solutions, if there are any, will be even more challenging.

Notes

1. The *New York Times* does write a compelling story conveying circumstantial evidence indicating that the worm may have been a joint United States/Israeli operative. See Broad, W., Markoff, J. and Sander, D., "Israeili Test Worm Called Crucial in Iran Nuclear Delay" (Janaury 15 2011) The *New York Times* available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (Accessed 7 February 2011). Many hacking sites, however, report that a dodgy company known as SERCO may be behind the attacks and have indicated that it is more likely that Stuxnet was released by a criminal malware group or by a company that does business with governments for defense contracts. See for example, "Is Serco behind Stuxnet" (thread started September 2010 and ongoing) available at http://www.abovetopsecret.com/forum/thread615788/pg1 (Accessed 7 February 2011).
2. The *New York Times* reports that retiring chief of Israel's intelligence agency, MOSSAD, has stated that Iran's nuclear power program has run into technical difficulties which will delay the nuclear program until 2015. Broad, note 83 above. The Iranian government has publicly announced that Stuxnet did not set back their nuclear program though there is aknowledgeable that there has been some disruption to Iranian centrifuges. This acknowledgement, however, does not specifically refer to Stuxnet. See for example, Madrigal, A., "Ahmadiejad publicly acknowledges Stuxnet disrupted Iranian centrifuges" (29 November 2010) available at http://www.theatlantic.com/technology/archive/2010/11/ahmadinejad-publicly-acknowledges-stuxnet-disrupted-iranian-centrifuges/67155/# (Accessed 7 February 2011).
3. Schneier, B., "Stuxnet" (October 7, 2010) available at http://www.schneier.com/blog/archives/2010/10/stuxnet.html (Accessed 7 February 2011). Similar descriptions may be found on all major anti-virus companies' websites. See for example Falliere, N., "Stuxnet introduces the first known rootkit for industrial control systems" (6 August 2010) Symantec available at http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (Accessed 7 February 2011). See also Microsoft, "The Stuxnet sting" (16 July 2010) available at http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx (Accessed 7 February 2011).
4. *See* report from the United States National Cyber-Forensics and Training Alliance on Stuxnet available at http://www.ncfta.net/ncfta-news/ncfta-cyber-alerts/stuxnet (Accessed 7 February 2011). A detailed video examining Stuxnet is provided by Langill, J., "Stuxnet worm detailed examination by SANS" available on a hacker website http://www.garage4hackers.com/showthread.php?604-Stuxnet-Worm-Detailed-Examination-by-SANS (Accessed 7 February 2011). Excellent information is also provided by Symanetc, note 85 above.
5. Jeremy Kirk, "Saudi Aramco restores internal network after malware attack" (20 August 2012) PC World available at http://www.pcworld.com/article/261461/saudi_aramco_restores_internal_network_after_malware_attack.html?tk=rel_news.

Canadian Foreign Policy Journal, 2013
Vol. 19, No. 2, 123–126, http://dx.doi.org/10.1080/11926422.2013.773543

Routledge
Taylor & Francis Group

Following in the footsteps of terrorism? Cybersecurity as a crowded policy implementation space

Nicole S. van der Meulen*

Department of Transnational Legal Studies, Faculty of Law, VU University Amsterdam

Keywords: cybersecurity; crowded policy space; European Union

The echoing call for a more secure cyberspace is heard around the globe. National cybersecurity strategies have become common practice as nation states sense the urgency to develop sufficient response capacities to deal with cybersecurity threats. As cybersecurity finds itself on top of many political agendas, its potential to be plagued by more common policy problems looms on the horizon. This commentary specifically addresses the issue of a crowded policy implementation space. The concept of a crowded policy space is most often associated with Majone (1986, p. 159), who coined the phase and described how "[i]n an already crowded policy space, solutions beget new problems, in the form of policy overlaps, jurisdictional conflicts and unanticipated consequences." The term has also been used in the context of the War on Terrorism, in particular in the European Union (EU), albeit from a slightly different perspective. The initial tendency at the European level, after the terrorist attacks of 11 September 2001, was to introduce new agencies and structures. The EU built these newly introduced formal initiatives on top of existing structures. As Den Boer (2006, p. 99) notes, "[w]ith this plethora of initiatives, the EU reinforced the already crowded policy space on counter-terrorism." The crowded nature in this sense is more a reflection of the growing number of actors involved in the development and subsequent implementation of policy, rather than crowded policies themselves. In essence, multiple actors emerge to implement the same or similar policies, leading to inefficiency.

In the field of cybersecurity, a similar reflex can be witnessed, both at the national as well as the supranational or European level. Just as the War on Terrorism led to the introduction of Europol and Eurojust, amongst others, cybersecurity led to the proposal to establish an EU Cybercrime Centre. In March 2012, the European Commission issued a press release stating its desire to introduce an EU Cybercrime Centre, to be hosted by Europol (European Commission 2012). The introduction of such a center seems logical, especially since the costs of cybercrime seemingly continue to increase. While the reliability of available figures remains a topic of discussion (see Anderson *et al.* 2012), a recent estimate claimed the global cost of cybercrime is US $110 billion per year (Symantec 2012). The complexity of attaching a reliable figure to

*Nicole van der Meulen completed a doctoral dissertation on financial identity theft at Tilburg University, the Netherlands, in 2010. Her manuscript was published by TMC Asser Press as Financial Identity Theft: Context, Challenges and Countermeasures. Afterwards, she worked as an information security advisor at GOVCERT.NL, the predecessor to the National Cyber Security Centre of the Netherlands. She currently focuses her research on cybersecurity developments and policy. Email: n.s.vander.meulen@vu.nl

the problem is enhanced through the different types of losses and costs associated with the problem, such as direct as well as indirect losses and defense costs (Anderson *et al.* 2012). Such a cybercrime centre, however, is certainly not the first organizational feature introduced within the broader scheme of cybersecurity. The EU already has ENISA, the European Network and Information Security Agency, which considers itself the EU's response to issues of cybersecurity. Moreover, on 1 June 2011, the EU Institutions set up a Computer Emergency Response Pre-configuration Team (CERT-EU). The European Commission committed itself to the launch of CERT-EU through its announcement in the Digital Agenda for Europe, adopted in May 2010. The creation of these new agencies might seem good initiatives at first, but they may, in fact, exacerbate existing problems within the EU. According to Klimburg and Tirmaa-Klaar (2011, p. 29),

> [t]he EU has approached the issue of cybersecurity in a fragmented manner, where parallel policies have sometimes been launched with different overlapping themes. Most of these initiatives have direct or indirect relevance to EU Members' preparedness to withstand serious cyberattacks, as they address the means and methods of cyberattacks, as well as the consequences of these attacks.

The fragmented approach identified by Klimburg and Tirmaa-Klaar refers to the existence of multiple organizations which are working on the topic of cybersecurity without much, if any, contact between them or even awareness of the others' existence. This leads to the existence of parallel policies, as well as parallel implementation or execution of policies. These developments illustrate how cybersecurity may head down a similar path as the War on Terrorism. Legislative, policy, development and intelligence activities with respect to cybersecurity are dispersed among various departments at the European level, hence the previously identified fragmentation. Examples of departments and institutions which are active with respect to cybersecurity include the European Parliament, Directorate-General Information Society and Media (DG INFSO)[1], Directorate-General Home Affairs (DG HOME), Directorate-General Enterprise and Industry (DG ENTR), the European External Action Service (EEAS) via the SITCEN (Joint Situation Centre, an EU intelligence body) and at the European Union Military Staff (EUMS), and the European Defence Agency (EDA), which is now appearing on the scene. As the European Organization for Security (EOS 2011) writes, "[t]hese critical challenges cannot be met with the existing and fragmented approach, and the cybersecurity strategy should be organised around two major dimensions:

(1) the federation of the different (and numerous) stakeholders;
(2) the consolidation of the different initiatives, at policy, governance, innovation and operational levels."

The consolidation can assist in the reduction of a crowded policy space and the increase of a more effective and efficient approach toward cybersecurity.

The EU is certainly not alone in this potential pitfall. As previously noted, many nation states introduced a cybersecurity strategy. According to the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCD CoE), a total of 18 countries have published a national cybersecurity strategy, as of August 2012. Simultaneous to this introduction, many also expressed the need to introduce new agencies responsible for cybersecurity. Moreover, cybersecurity councils, albeit on a more limited basis, were also introduced to cover the more policy-oriented aspects of the problem. This is, according to Klimburg and Tirmaa-Klaar (2011), necessary. They argue how besides operational components, such as more advanced versions of Computer Emergency Response Teams (CERTs), there must also be relevant policy bodies which are able to interface directly with political leadership at the highest levels.

Even so, as cybersecurity continues to increase in importance, everybody appears to want a piece of the pie. As the Canadian strategy (Public Safety Canada 2010, p. 9) rightfully notes, "[w]ith a subject as critical as cybersecurity, there is no room for ambiguity in terms of who does what." This is a fundamental tenet of Critical Infrastructure Protection, and essential to establishing accountability for complex systems, such as Critical Infrastructures. The risk of ambiguity, however, is certainly present due to the tendency to develop a crowded policy arena with overlapping actors. Moreover, the risk is exacerbated since cybersecurity inherently appears subject to a crowded policy implementation space. Cybersecurity implicates a wide variety of policy areas, as cyber itself is an aspect present in nearly all activities in contemporary society. Furthermore, information technology (IT) and Telecom is a National Critical Infrastructure (NCI) in itself, as well as a supporting capability for most of the other nine NCIs. The diversity of threats demonstrates how the implications of cyberinsecurity are broad and as such applicable to a variety of actors. This leads to another challenge particularly essential to discuss within the confines of this commentary: the issue of policy ownership. As the threat toward nation states increases, especially due to incidents such as Stuxnet and the increasing threat of digital espionage, cybersecurity has become an issue of national security – and rightfully so. However, cybersecurity is more than that. Other levels of government must not be forgotten. This may sound contradictory to the previous warnings issued to prevent cybersecurity from becoming a crowded policy space, but it is not. Local, state and federal levels of government must deal with cybersecurity, but from differing perspectives. The evolving possibilities with respect to e-government, for example, provide different challenges than a looming cyberwar. As a result, there is no exclusive policy ownership over the issue of cybersecurity. All of its facets must be covered and, more importantly, coordinated. Without, obviously, developing overlaps between policy implementers, which makes coordination essential. The tendency, therefore, is to introduce overarching agencies.

The description provided by the German cybersecurity strategy of its National Cyber Response Center best seems to connect to the necessity of a coordinator to prevent ambiguity about role distribution. This is the entity that will tie the disparate cyberprotection programs together to provide a common operating picture and a consistent threat picture. No command and control hierarchy is implied; rather, it is one of collaboration among colleagues and specialists. In its strategy, the German government (Federal Ministry of the Interior 2011, p. 8) describes how:

> To optimize operational cooperation between all state authorities and improve the coordination of protection and response measures for IT incidents we will set up a National Cyber Response Centre... Quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators enables the National Cyber Response Centre to analyse IT incidents and give consolidated recommendations for action.

Certain states explicitly mention the transformed or new agency is to function as a coordinator. The Australian government states in its strategy how CERT Australia will be the national coordination point within the Australian Government (Australian Attorney General 2009). In particular, CERT Australia is responsible for the provision of cybersecurity information and advice for the Australian community. CERT Australia is also to be the official point of contact in the expanding global community of national CERTs to support more effective international cooperation.

The importance of international cooperation requires states to be clear about the primary point of contact for other states. A crowded policy implementation space can lead to internal competition and problems, which may also hinder international cooperation, a vital component of any integral approach to cybersecurity. What must be borne in mind as the developments on

cybersecurity move forward is that sometimes less is more – or, rather, fewer actors can do more work due to greater efficiency. And that success is as much, if not more, about actions as it is about actors.

Note

1. As of 25 April 2012 this has become Directorate-General Connect.

References

Anderson, R., *et al.*, 2012. *Measuring the cost of cybercrime.* Workshop on the Economics of Information Security (WEIS) [online]. Available from: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf [Accessed 10 December 2012].

Australia Attorney General, 2009. *Cyber Security Strategy* [online]. Available from: http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy [Accessed 1 October 2012].

Den Boer, M., 2006. Fusing the fragments: challenges for EU internal security governance on terrorism. *In*: D. Mahncke and J. Monar, eds. *International terrorism: a European response to a global threat.* Brussels, Belgium: P.I.E. Peter Lang Publishing, 83–113.

European Commission, 2012. *An EU cybercrime centre to fight online criminals and protect e-consumers* [online]. Available from: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317 [Accessed 1 October 2012].

European Organization of Security (EOS), 2011. Steps towards implementing a European cyber-security strategy [online]. Available from: http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf [Accessed 1 October 2012].

Federal Ministry of the Interior, 2011. *Cybersecurity strategy for Germany* [online]. Available from: http://www.cio.bund.de/SharedDocs/Publikationen/DE/ITSicherheit/css_engl_download.pdf?__blob=publicationFile [Accessed 1 October 2012].

Klimburg, A. and Tirmaa-Klaar, H., 2011. *Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU* [online]. Available from: http://www.evi.ee/lib/cyber.pdf [Accessed 1 October 2012].

Majone, G., 1986. *Evidence, argument, & persuasion in the policy process.* New Haven, CT: Yale University Press.

Public Safety Canada, 2010. *Canada's cybersecurity strategy: for a stronger and more prosperous Canada.* Available from: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf [Accessed 1 October 2012].

Symantec, 2012. 2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually [online]. Available from: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 [Accessed 10 December 2012].