

2015-2016

Graduate Research Awards

for Disarmament, Arms Control and Non-Proliferation



AWARD WINNERS SEMINAR

Global Affairs Canada Headquarters
Lester B. Pearson Building, Ottawa, Canada
February 26, 2016

A joint project of:



and the **International Security Research and Outreach Programme**
Global Affairs Canada

Executive Summary

The ***Graduate Research Awards for Disarmament, Arms Control and Non-proliferation*** (GRA) programme was initiated in 2003 by Dr. Jennifer Allen Simons, President of The Simons Foundation, in partnership with the [International Security Research and Outreach Programme \(ISROP\)](#) of Foreign Affairs and International Trade Canada (now [Global Affairs Canada](#)). The primary objective of the Awards is to enhance Canadian graduate level scholarship on non-proliferation, arms control and disarmament (NACD) issues.

Since its inception, the Graduate Research Awards programme has provided over \$285,000.00 in scholarships to Canadian graduate students working on policy-relevant NACD issues and has helped to encourage a new generation of young Canadian scholars dedicated to further expanding their knowledge and expertise on these critical issues.

The original programme offered three Doctoral Research Awards of \$5,000.00 and four Master's Research Awards of \$2,500.00 each year to support research, writing and fieldwork leading to the completion of a major research paper or dissertation proposal on an issue related to disarmament, arms control and non-proliferation.

In order to allow a greater number of students to participate, the GRA competition was later restructured to consist of a series of debates on timely issues. The eight students who made the strongest argument in support of their position, as determined by an expert review panel, were selected to receive a Graduate Research Award of \$3,000.00 and required to defend their position in person at the GRA Debates held at the Department of Foreign Affairs headquarters in Ottawa.

The 2015-2016 competition has been revised to simplify the application process and increase the value of the cash awards. A total of four awards of CAD\$5,000 were available to Canadian Master's and/or Doctoral candidates to support the research and writing of an academic paper responding to a specific Non-Proliferation, Arms Control and Disarmament (NACD) topic. Awards also included travel support to Ottawa where successful candidates presented their completed papers during a special seminar held at Global Affairs Canada headquarters on February 26, 2016.

The GRA Seminar in Ottawa provided a unique opportunity for exchange among departmental officials, Canadian opinion-leaders and the next generation of experts in the NACD field. International Security and Political Affairs and Non-Proliferation and Disarmament Division officials attended the sessions and Global Affairs Canada hosted a lunch in honour of the GRA recipients following the presentations.

This year, students were given the option of writing on the following topics:

Master's Candidates:

1. *What role could Article 36 of the Additional Protocol (I) of the Geneva Conventions and the requirement for weapon reviews play in addressing new and emerging technologies, such as lethal autonomous weapons systems?*
2. *Space Security and Cyber Security: What are the common issues and challenges associated with cyber security and space security? What types of solutions could be offered to these challenges?*

Doctoral Candidates:

3. *Improving Canada's counter-proliferation architecture: what policy proposals/legislative amendments could be developed to close Canada's remaining counter-proliferation gaps?*
4. *Which approach is more likely to achieve a world without nuclear weapons – the immediate negotiation of a Nuclear Weapons Convention OR pursuing a step-by-step process to negotiate and implement complementary legal instruments and political agreements, like the NPT, the CTBT, an FMCT, etc.?*

We are pleased to congratulate the following 2015-2016 Graduate Research Awards recipients who each received a cash award of \$5,000.00 from The Simons Foundation and travel support to Ottawa to participate in the GRA Seminar:

- Kieran Alkerton – Munk School of Global Affairs, University of Toronto
- Daniel Golston – Fitzwilliam College, University of Cambridge
- Sacha Lavoie-Guilini – Graduate School of Public and International Affairs, University of Ottawa
- Jenny Yang – Darwin College, University of Cambridge

We also wish to recognize James McNee of Global Affairs Canada's International Security Research and Outreach Programme and Elaine Hynes of The Simons Foundation for their work to coordinate and execute the programme this year.

The 2016-2017 Graduate Research Awards competition will be launched in fall 2016.

Disclaimer: The views and positions expressed in this report are solely those of the author and do not necessarily reflect the views of The Simons Foundation or Global Affairs Canada. The report is in its original language.

Copyright remains with the author or the GRA programme. Reproduction for purposes other than personal research, whether in hard copy or electronically, requires the consent of the author(s). If cited or quoted, please ensure full attribution to source material including reference to the full name of the author(s), the title of the paper, the date, and reference to the Graduate Research Awards programme.

Contents

Opening Remarks	i
Martin LarRose, Director, Non-Proliferation and Disarmament Division Global Affairs Canada	
Opening Remarks	4
Jennifer Allen Simons, C.M., Ph.D., LL.D., Founder and President The Simons Foundation	
Graduate Research Award Presentation 1	8
Jenny Yang Master's, International Relations, Darwin College, University of Cambridge	
Graduate Research Award Presentation 2	12
Sacha Lavoie-Guilini Maîtrise, affaires publiques et internationales, Université d'Ottawa	
Graduate Research Award Presentation 3	16
Kieran Alkerton Master's, Munk School of Global Affairs, University of Toronto	
Graduate Research Award Presentation 4	20
Daniel Golston Master's, International Relations and Politics, University of Cambridge, Fitzwilliam College	
Keynote Address	25
Bruce G. Blair, Ph.D. Co-Founder, Global Zero and Research Scholar, Program on Science and Technology, Princeton University	
Expert Review Committee	34
Annex 1: 2015-2016 GRA Seminar Agenda	35
Annex 2: 2015-2016 GRA Competition Details	36

Opening Remarks

MARTIN LAROSE

Director, Non-Proliferation and Disarmament Division
Global Affairs Canada

Good morning / Bonjour.

On behalf of the Department's International Security Research and Outreach Programme, and the Non-Proliferation and Disarmament Division, we are pleased to welcome you to the 2015-16 Graduate Research Awards.

These awards have long been a key component of the Department's academic outreach in this area, and we are pleased to have you all here and to hear presentations on your winning papers.

L'objectif de ces bourses est de former la prochaine génération de chercheurs canadiens sur des enjeux liés à la sécurité internationale, notamment la non-prolifération, le contrôle des armements et le désarmement.

In 2003, Dr. Simons created the Graduate Research Awards for Disarmament, Arms Control, and Non-Proliferation, along with the Department's International Security Research and Outreach Programme.


Since its inception, the Graduate Research Awards programme has provided over \$240,000.00 in scholarships to Canadian graduate students working on policy-relevant non-proliferation, arms control and disarmament (NACD) issues and has helped to encourage a new generation of young Canadian scholars dedicated to further expanding their knowledge and expertise on these critical issues.

I would especially like to welcome the four recipients of this year's awards:

- Jenny Yang and Daniel Golson from the University of Cambridge,
- Sacha Lavoie-Guilini from the University of Ottawa, and
- Kieran Alkerton from the University of Toronto.

Congratulations on your winning papers, and thank you for the significant work you have done to prepare for today's event. Your efforts exemplify what the GRA attempts to achieve, and we hope that these awards will continue to inspire your academic engagement on the important issues of disarmament, arms control, and non-proliferation in future years.

Let me also acknowledge Dr. Jennifer Simons for her continued leadership on these issues and for the Simons Foundations' continued support of the Graduate Research Award program.



In addition, I have the distinct pleasure to welcome Dr. Bruce Blair, co-founder of Global Zero, who the Simons Foundation has kindly arranged to speak to us today.

Before I provide further details on the format of today's discussion, I thought it would be helpful to provide some context on why emerging technologies and issues such as lethal autonomous weapons systems, as well as space and cyber security, were selected as themes for this year's Awards.

Lethal autonomous weapons systems--also known as "killer robots"--are garnering increasing attention worldwide. Though fully autonomous weapons systems do not yet exist, rapid technological advancements compel the international community to examine the potential implications of such weapons systems and examine ways to find a common approach to address this emerging technology.

Article 36 of the Additional Protocol I of the Geneva Conventions is one potential avenue to begin to address lethal autonomous weapons systems moving forward.

Space security, and more particularly the security of the space infrastructure upon which Canada heavily relies, is a prominent feature of the department's work on space issues.

In particular, my division is responsible for administering the Remote Sensing Space Systems Act, which establishes a licensing regime aimed at securing sensitive data transmitted from space, and seeks to strike an appropriate balance between security and commercial interests in space.

Space infrastructure is vulnerable to a number of threats, including hostile acts such as cyber-attacks. At the same time, the lack of clear norms governing many aspects of space activities, the inherent difficulties in establishing such norms given the characteristic of outer space as an area of global commons, and the low level of trust amongst space-faring nations, all pose real challenges to our efforts to manage these threats effectively both at the national and international level.


Drawing links between cyber and space security, two domains which share similarities in the nature of their challenges, can contribute to our understanding of the space security environment and help identify solutions to manage threats and set clearer and better norms of behavior in space.

In delivering your presentations, we encourage you to keep to the 10 minutes allotted to each speaker, so that we leave enough time for questions.

Following the presentations and Q&A, we will have the distinct pleasure to welcome Dr. Bruce Blair, co-founder of Global Zero, who will give a 15 min presentation.

This event will take place under Chatham House Rule, meaning that any remarks made here are not for attribution.

I will conclude by now formally introducing to you, Dr. Jennifer Simons.



Dr. Jennifer Allen Simons is the President of The Simons Foundation, based in Vancouver. Through the Foundation's work, Dr. Simons has been a leader in research, advocacy, and action to advance a number of important issues, including; nuclear disarmament, peace, human rights, and global cooperation.

As I mentioned earlier, Dr. Simons created the Graduate Research Awards for Disarmament, Arms Control, and Non-Proliferation in 2003, in partnership with the Department's International Security Research and Outreach Programme. Since 2003, the Simons Foundation has continued to provide scholarships annually to Canadian students pursuing Masters and PhD. studies on arms control and disarmament issues.

Today's event serves as a testament to the continued value of our collaboration. We are proud to welcome Dr. Simons for another productive meeting here in Ottawa.

Dr. Simons, the floor is yours.

Opening Remarks

JENNIFER ALLEN SIMONS, C.M., PH.D., LL.D.

Founder and President

The Simons Foundation

Good Morning,

Martin, it is a pleasure to see you again, and I add my welcome to yours. I would like to thank James McNee, of Global Affairs Canada, and Elaine Hynes from The Simons Foundation for their excellent organization and management of this programme.

It is a pleasure to be here participating again in the annual Graduate Research Awards seminar, a programme which the International Security Research and Outreach Programme of Global Affairs Canada and The Simons Foundation have partnered for fourteen years.

The joint programme was forged in 2003, during the Liberal era – liberal in every sense, with the Cold War over and a time of hope for global peace and disarmament – a time when Canada's Foreign Policy was grounded in Human Security, and civil society partnerships and civil society contributions were welcomed by government.

The year before this programme began, The Simons Foundation initiated, funded and partnered with Global Affairs Canada (then Foreign Affairs) in another programme - a conference at the United Nations in Geneva on Space Security. The Simons Foundation has continued to sponsor these annual conferences. And Paul Meyer, former colleague of many of you, who is now Senior Fellow at The Simons Foundation and responsible for the Foundation's Space Security Programme, participates in the agenda development of these events.

Following the first conference, the Department initiated and funded a Space Security Index Project, headquartered at Project Ploughshares. Unfortunately, the Canadian government withdrew its funding and my hope is that – because of the growing importance of security in space, and the potential for cyber warfare, that the Government will return to this important project.

During the past few years, I have noted the lengths to which the department has gone to maintain the Graduate Research Awards programme – despite the financial hollowing out of the department. And I commend the members of the Department for their efforts to retain it. Because of these constraints, the programme has undergone continual financially downward-driven modifications and it is my hope that we can restore it to its earlier health and provide awards to more students in order to continue to develop a Canadian community of disarmament scholars, and to disseminate the understanding of the contribution that disarmament would make to a peaceful and economically healthy world.

There are few educational initiatives in schools and universities for research and education on the negative effects of weapons – from handguns to nuclear weapons to 21st century weaponry - necessary to counter one of the most lucrative of all businesses, benefiting corporations and government who profit from the sale of these purveyors of death.

Disarmament education is an essential requirement in the modern world but remains a lacuna in educational institutions – a gap I been attempting to fill in Canada for the last 15 years; and am pleased that there will be a new Simons Chair in Disarmament, Global and Human Security at the Liu Institute at the University of British Columbia - the only Disarmament Chair in Canada.

I am very happy that there are students pursuing with this subject. And I congratulate the recipients of the Graduate Research Awards, and commend you for your choice of study - for your specialization in Space and Cyber Security and 21st century's weapons and warfare.

Cyber warfare and the utilization of autonomous weapons raise the level of the likelihood of a nuclear catastrophe - a horrifying prospect given the possibilities of hacking into the nuclear command and control systems, and of autonomous weapons tracking previously invisible nuclear submarines. This type of warfare and these weapons bring closer the possibility of a nuclear detonation through accident, miscalculation or malicious intent which could trigger a nuclear war.

The political and security environment has changed radically since the early 2000s. The atmosphere at the recent Munich Security Conference was one of depressing awareness of the myriad of crises with which the world is faced. Moreover the negative Russia-NATO rhetoric was alarming. It is imperative in the interests of global security that the channels for dialogue between Russia and the West are kept open - especially so because, as Russia's newly grim-faced, Prime Minister Medvedev in Munich said the world has "slipped into the era of a new Cold War" and he laid the blame – as did all the Russians present - on NATO!

It is extremely important to make some headway on stalled nuclear disarmament process - thus essential that we remain in dialogue with Russia before the situation spirals out of control. All the nuclear weapons states are engaged in expensive modernizations of their arsenals with Russia determined - despite its poor economic status - to keep even with the United States. Both countries have increased the number of deployed warheads; and have an estimated 1,800 nuclear weapons on high alert status. Possession of nuclear weapons is considered to be more dangerous now than during the Cold War. And given the tension between the U.S. and Russia, and NATO and Russia, it is quite likely that there could be an inadvertent nuclear exchange.

The possibilities for nuclear disarmament at this time *seem* questionable. Yet is not a lost cause, and creative thinking is required in order to further positive change in the disarmament area.

In the Liberal years at the end of the 1990s Canada introduced language on "nuclear disarmament" to the NATO documents. In fact, The Simons Foundation bestowed its Award for Distinguished Global Leadership on Lloyd Axworthy for initiating this action. Given Russia's current aggression and the flaunting of its nuclear option, it seems that the political and security environment is not right for any further action to change NATO's circular argument that ***as long***

as nuclear weapons exist, it will remain a nuclear alliance. However, there are steps that can be taken.

Mr. Dion has stated his intention to re-engage with Russia. Canada building on its 1990s success could encourage the United States and NATO to adopt Global Zero's plan – which Dr. Blair may have time to talk about - to eliminate the United States tactical weapons from Europe with an agreement from Russia to remove its NATO-border tactical nuclear weapons to storage facilities in Russia. High-level US military leaders consider these weapons redundant and serve no purpose. NATO would remain a nuclear alliance because of the nuclear United Kingdom and France, as well as the United States strategic nuclear weapons based on land and in submarines.

Canada's commitment to nuclear disarmament is grounded in the Nuclear Non-Proliferation Treaty and to a series of steps – the step-by-step approach - to disarmament. But one must ask how long are Canada and other like-minded states prepared to wait for the United States and China to ratify the CTBT and for others to follow? And how long are Canada and other like-minded states prepared to wait for Pakistan to decide that it has enough nuclear weapons and to agree to remove its opposition to the FissBan Treaty? And how long are Canada and other like-minded states prepared to wait for the nuclear weapons states outside the NPT to join as non-nuclear weapon states? This step-by-step approach is in a state of paralysis with no resolution in sight.

The NPT has been praised as a successful curb to proliferation of nuclear weapons but this is not enough! North Korea has demonstrated the weakness of the NPT.


There are avenues for Canada to pursue initiatives within the NPT which will further the goal of a nuclear free world.

Canada is one of the 193 United Nations member-states participating in the Humanitarian Impact of Nuclear Weapons meetings but has, to date, not signed the Austrian- initiated Humanitarian Pledge. This is disappointing because Austria has made quite clear the separation of their initiative from the Nuclear Weapons ban approach – a ban which would become a continuation of the same old story as with the NPT - the non-nuclear weapons states held hostage by the nuclear weapons states

It is my hope that Canada will sign the Humanitarian Pledge, become more active and forward-thinking and exert its influence to encourage the P-5 states to join in these discussions and participate in the Open-Ended Working Group because until the nuclear weapons states do, not much can be achieved.

Mr. Dion has signalled that Canada also intends to re-engage with Iran. There is an opportunity for Canada within its NPT commitment to further disarmament and as well to rebuild relations with Iran – to undo some of the damage caused by the previous government.

Last year at the NPT Review Conference, and again at the UN General Assembly Canada, voted **against** the Resolutions on steps towards establishment of a zone free of weapons of mass destruction in the Middle East which, since 1995, in essence, is the fourth pillar of the NPT.



On July 31st of last year Iran Foreign Minister Zarif made a call in The Guardian newspaper for the “joint comprehensive plan of action” concluded by Iran and the P-5 + 1 which “cements Iran’s status as a zone free of nuclear weapons” to be expanded “to encompass the entire Middle East.”

Members of the Princeton Program on Science and Global Security - of which Dr. Blair is a member - have developed a step-by-step concrete plan to fulfil this objective. For Canada to approach Iran in support of this resuscitation of the establishment of an “effectively verifiable Middle East Zone Free of Nuclear Weapons of Mass Destruction” would be a non-tendentious act of supportive diplomacy.

It is of upmost importance to keep the dialogue going with Russia and Iran and now that ***Canada is back***, the country can return to its forward-looking, hopefully pro-active, diplomatic multilateral policy.

Thank you very much!

Graduate Research Award Presentation 1

JIAOLI (JENNY) YANG

Master's

International Relations

University of Cambridge

Jenny Yang is a Junior Research Fellow for the NATO Association of Canada, pursuing her Master's degree (MPhil) in International Relations at the University of Cambridge. She has previously worked at INTERPOL headquarters in Lyon, France as a Junior Analyst in the Strategic Planning Directorate. Her interest in arms control comes from having worked on Syrian chemical weapons disarmament, in which she provided support to the Canadian Permanent Representation to the Organisation for the Prohibition of Chemical Weapons (OPCW). She was named a NATO's Future Young Leader by the Atlantic Council of Germany in 2014 and has represented Canada at international security-related conferences in Kosovo, Bosnia-Herzegovina, Spain, and Wales.

TOPIC: What role could Article 36 of the Additional Protocol (I) of the Geneva Conventions and the requirement for weapon reviews play in addressing new and emerging technologies, such as lethal autonomous weapons systems?

How to Stop Killer Robots: The Role of Weapons Review in the Regulation of Autonomous Weapons Systems

"They don't get hungry. They're not afraid. They don't forget orders. They don't care if the guy next to them has just been shot. Will they do a better job than humans? Yes."

- Gordon Johnson, former member of the Pentagon Joint Forces Command (Foy 52)

At first glance, the futuristic concept of lethal machines governed by artificial intelligence appears to belong more in the realm of science fiction than reality. The International Committee of the Red Cross (ICRC) defines Autonomous Weapons Systems (AWSs) as weapons able to select and attack targets in the absence of human intervention (Boulain 9). According to *Mines Action Canada*, AWSs are already being developed and tested in countries such as China, Russia, South Korea, Israel, the United Kingdom, and the United States (Lacroix-Wilson Postmedia). Worldwide, there are currently fifty non-governmental organizations participating in the Global Campaign to Stop Killer Robots (ibid.). In the case of Canada, the Department of National Defence denies that it has contracted any research on autonomous weapons systems (ibid.). In spite of these claims, robotics development reports indicate that more than fifty countries are in the process of developing AWSs — including Canada (Foy 51).

In light of the proclivity of technological innovation to outpace legal regulation, this essay will explore the role of weapons review — particularly Article 36 of the Additional Protocol (I) of the Geneva Conventions — in the regulation of AWSs. Through identifying weaknesses in the current weapons review process such as a lack of formal review mechanisms in countries, state secrecy, passivity, and complexity, this essay hopes to draw attention to the various solutions to be discussed in detail below.

At present, official statements by most governments insist on the defensive applications of autonomous weapons systems. However, according to Christof Heyns, the UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, it is important to remember that airplanes and drones were first used exclusively for the purpose of surveillance (as cited in Roff 211). To quote Heyns, “Subsequent experience shows that when technology that provides a perceived advantage over an adversary is available, initial intentions are often cast aside” (ibid.).

The benefits of AWSs on the battlefield are manifold. Machines are able to perform tedious tasks reliably for long periods of time, without the need to eat or sleep. AWSs are able to provide area denial without the physical presence of forces, freeing up combat capability (Backstrom & Henderson 488). Compared to human-operated weapons, AWSs are ultimately more cost-effective (Foy 52). Machines are also able to make decisions quickly and consistently, shortening the Observe, Orient, Decide, and Act (OODA) loop (Backstrom & Henderson, 491). Given the ability to function in the absence of continuous communication with central command, AWSs are less vulnerable to cyberattacks than ‘in the loop’ remotely controlled weapons (Foy 52). Above all, machines are immune to the fog of war and do not fall prey to psychological biases such as Scenario Fulfillment, defined as the fitting of new information to pre-existing beliefs (ibid.).

The advantages of autonomous weapons systems coupled with the pace of technological innovation raises several important questions. What is the current state of affairs of the legal framework responsible for regulating AWSs? More importantly, is the existent legal framework able to safeguard the principles and spirit of the law of armed conflict? To determine lawfulness of the weapon system in question, the Geneva Conventions dictate that the weapon must: i) first, not be indiscriminate by nature and ii) second, refrain from causing unnecessary suffering or injury (as cited in Thurnher; Boothby 108). In order to ensure compliance with the aforementioned rules, Article 36 of Additional Protocol I indicates that states must conduct a legal review of weapons “before they are developed, acquired, or otherwise incorporated into a State’s arsenal” (Casey-Maslen 413). Though undeniably useful, weaknesses implicit in the implementation of Article 36 include a lack of formal review mechanisms in various countries, state secrecy, passivity, and complexity.

First of all, more than three decades after Protocol I’s adoption, the number of countries known to have set up formal review mechanisms for new weaponry remains minimal (Rappert et al. 781). Weapons review faces a free riding problem, with smaller states relying on larger states to conduct weapons reviews, shirking their obligation to independent review (Rappert et al. 781). Only seven countries (Australia, Belgium, the Netherlands, Norway, Sweden, the U.K., and the U.S) have both confirmed formal review processes and have made these processes publically available (ibid.). Canada counts among the thirteen countries¹ indicating that they may have formal or informal review mechanisms, though there is insufficient information available to confirm whether this is the case (ibid.). The obvious solution here would be to heighten transparency by urging countries to make their formal weapons review processes

¹ Formal: Canada, Czech Republic, New Zealand, Russian Federation, Switzerland; Informal: Austria, Brazil, Croatia, Finland, Mexico, Poland, Portugal, and South Africa (Rappert et al. 781)

public and also encouraging smaller countries to conduct independent weapons reviews. These aims may be met through establishing an international body to create robust information sharing networks. Another approach would be the use of force-multipliers such as academia and NGOs to frame the public debate and draw attention to concerns vis-à-vis emerging technology.

Second of all, even within countries, the highly classified nature of a weapon's capability means that lawyers, engineers, and operators face difficulties in overcoming state secrecy requirements and compartmentalized access (Backstrom & Henderson 513). Between countries, information sharing is even more difficult. Because Article 36 does not require states to make their weapons review processes public, other contracting states face difficulties in verifying compliance (Rappert et al. 781). The nature of state secrecy also exacerbates the unpredictability of AWSs in armed conflict. According to Peter Asaro, because countries guard their codes and algorithms from prying eyes, it is almost impossible to predict how adversarial systems will actually behave on the battlefield (as cited in Lacroix-Wilson).

According to Boulanin, though states might not wish to share information on individual weapons reviews, they could be convinced to share procedural details about their review mechanisms in order to prove their commitment to weapons review (18). One innovative solution proposed by Backstrom & Henderson is to develop legal parameters that can be subject to systems testing (513). Another alternative solution would be to employ what Backstrom & Henderson refers to as "multi-parameter acceptance criterion equation sets." Though complex, such equation tests would facilitate hypothesis testing, simultaneously taking into account data on reliability, confidence bounds, and risk factors (ibid.).

The third issue seems to be that Article 36 is reactive in its terms given that it fails to specify any particular mode of compliance (Rappert et al. 781). One measure to enhance proactivity proposed by Backstrom & Henderson is especially promising. Instead of passively receiving test results, during the test and evaluation phases of new weapons, lawyers would identify areas of legal concern, which could be made testable (509). Data obtained would be cross-referenced against existing data on weapons reliability to enhance the decision-making process, when considering a new targeting procedure, for instance (ibid.)

Last but not least, weapons systems are growing in complexity, often leading to unforeseen events (Boulanin 12-13). The range of skills required to understand a sword differ from the skills required to understand a Predator or Reaper drone. To evaluate modern weaponry, the review board would need knowledge of design, manufacturing, production, and testing methods as well as how the weapon is employed in combat. Lack of capability within the review body to adequately understand all the facets of the technology being examined poses a significant hurdle (Rappert et al. 782). Ultimately, computer scientists, engineers, and lawyers must engage with one another in critical discussion when a state conducts an Article 36 weapons review (Backstrom & Henderson 513). Lawyers in particular must fully understand the operational applications of a weapon, using this knowledge to build robust operational guidelines compliant with international humanitarian law.

In closing, due to technological innovation and increasingly postmodern, non-linear, ambiguous battle spaces, it is becoming more difficult to verify that a new autonomous weapons system meets the requirements of international humanitarian law, as required by Article 36 (Asaro 693). Certain weaknesses ingrained in Article 36 discussed above could be countered by promoting wider adoption of formal review mechanisms, information-sharing, greater multidisciplinary among review bodies, and taking a more proactive stance on weapons review.

However, fundamentally, the very nature of international humanitarian law presupposes that the combatants will be human (Asaro 670). From a moral vantage point, what Roff terms “killing by machine” fails to uphold the dignity of the person being killed (214). No moral relationship can exist between a machine and its human target. In deploying AWSs, the message sent to the target population is that their lives are not worth placing even one soldier in harm’s way (Roff 214). In reducing costs for the attacker, AWSs may very well have unintended consequences such as lowering the threshold for armed conflict and engendering instability. At its core, ethical values must guide the design of new and emerging weaponry. Until we understand more about the ramifications of artificial intelligence and autonomous weaponry, the precautionary principle as advocated by John Sullins justifies a ban on the production and use of autonomous weapons systems (11).

BIBLIOGRAPHY

Asaro, Peter. “On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making.” *International Review of the Red Cross*. 94. 886 (2012): 687-709. Print.

Backstrom, Alan. Henderson, Ian. “New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews.” *International Review of the Red Cross*. 94. 886. 2012: 483-514. Print.

Boothby, William. “Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors.” Surrey: Asser Press, 2014. Print.

Boulanin, Vincent. “Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems.” *SIPRI Insights on Peace and Security*. No. 2015. 1 (2015): 1-28. Print.

Casey-Maslen, Stuart. “Weapons Under International Human Rights Law.” Cambridge: Cambridge University Press, 2014. Print.

Foy, James. “Autonomous Weapons Systems: Taking The Human Out Of International Humanitarian Law.” *Dalhousie Journal of Legal Studies*. 23.47. 2013: 47-70. Print.

Lacroix-Wilson, Jeff. “Canada versus Killer Robots.” *Ottawa Citizen*. April 29, 2014. Print.

Rappert, Brian. Moyes, Richard. Crowe, Anna. Nash, Thomas. “The Roles Of Civil Society In The Development of Standards Around New Weapons and Other Technologies of Warfare.” *International Review of the Red Cross*. 94.886 (2012): 765-785. Print.

Lawland, Kathleen. Coupland, Robin. Herby, Peter. “A Guide to the Legal Review of New Weapons, Means and Methods of Warfare.” *International Committee of the Red Cross*. Geneva, ICRC: 2006. Print.

McClelland, Justin. “The review of weapons in accordance with Article 36 of Additional Protocol I.” *RICR*. 85. 850 (2003): 397-415. Print.

Roff, Heather. “The Strategic Robot Problem: Lethal Autonomous Weapons in War.” *Journal of Military Ethics*. 13.3 (2014): 211-227. Print.

Sullins, John P. “An Ethical Analysis of the Case for Robotic Weapons Arms Control.” *5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2013. Print.

Graduate Research Award Presentation 2

SACHA LAVOIE-GUILINI

Maîtrise en affaires publiques et internationales
Université d'Ottawa

Sacha Lavoie-Guilini is a first year student at the University of Ottawa in Public and International Affairs. He has previously completed a Bachelor's degree in Political Science at the University of Ottawa. His interests are focused on International Security issues and National Security. The subject of his Master's Thesis will be on the implications and causes of the pledging allegiance process by which terrorism networks are created and perpetrated. In the Fall of 2016, he will be part of a student exchange at the Paris School of International Affairs, where he will have the chance to develop new perspectives on his thesis subject.

TOPIC: What role could Article 36 of the Additional Protocol (I) of the Geneva Conventions and the requirement for weapon reviews play in addressing new and emerging technologies, such as lethal autonomous weapons systems?

L'article 36 du Protocole (I) additionnel de la convention de Genève a été implanté pour offrir une solution aux développements futurs de l'armement militaire. Plus spécifiquement, l'objectif était de formuler une approche proactive pour réguler tout développement dans l'armement militaire en assujettissant l'armement aux lois humanitaires internationales :

« Dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, une Haute Partie contractante a l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante. »²

Par contre, il fallait encore développer un cadre légal à partir duquel une « Haute Partie contractante » devait statuer qu'un armement n'était pas en accord avec les principes du droit international. C'est dans cette optique que fut adoptée en 1980 la « Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination »³. Cette convention se retrouve dans l'alinéa (b) de l'Article 35 du Protocole additionnel I. L'élaboration d'une nouvelle arme doit donc prendre en considération les effets

²Comité International de la croix rouge, « Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977. », <https://www.icrc.org/dih/WebART/470-750045?OpenDocument>.

³ Comité International de la croix rouge, « Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination. Genève, 10 octobre 1980 », https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-2&chapter=26&lang=fr&clang=_fr

traumatiques excessifs de son utilisation ainsi que sa capacité à frapper avec (ou sans) discrimination. En plus de ce cadre légal, il faut aussi que le nouvel armement puisse satisfaire les normes traditionnelles en matière de déroulement d'un conflit, soit la distinction (Art. 48), la proportionnalité (Art 51&57) et les précautions possibles avant l'attaque (Art.57). L'article 36 permet donc de « filtrer » le nouvel armement à travers les normes créées pour limiter les dommages collatéraux importants et la souffrance inutile en plus de permettre la révision de l'armement pour qu'il soit en accord avec le droit international traditionnel. Restait à savoir qui serait responsable de faire respecter ces normes. Lors de l'élaboration de la l'article 36 du Protocol I additionnel de la convention de Genève de 1949, il y eut des propositions relatives à la création d'une agence centrale qui serait chargée de s'occuper de la révision de l'armement. Par contre, cette proposition a rapidement été écartée pour des motifs sécuritaires, du rejet de l'ingérence internationale et de la pluralité des approches possibles dans la révision de l'armement (McClelland, 2003, p.414). L'approche privilégiée est donc immanquablement une supervision nationale de l'armement.

Les pays développant de l'armement militaire se rapprochant des « lethal autonomous weapons systems » seraient en théorie responsable de la lourde tâche de faire respecter le droit international dans l'élaboration de ce nouvel armement. Plusieurs avenues pourraient alors être employées. McClelland (2003) note une multitude de processus que pourraient employer les pays pour la révision du nouvel armement, et ce, à chaque étape de l'élaboration de l'armement en question. À cet effet, les pays pourraient employer des comités de révisions et des experts légaux en terme de droit international qui seraient chargés d'analyser un ensemble de données provenant de domaines d'expertises variés, allant des rapports scientifiques jusqu'à la documentation fournis par le fabricant (McClelland, 2003). Il nous faut alors mentionner quelques difficultés importantes auxquelles ce type de révision devra faire face. Notamment, les experts vont devoir prouver que ces systèmes sont dotés d'une intelligence artificielle suffisamment avancée pour prendre toutes les précautions possibles avant l'attaque pour ne pas causer de dommages collatéraux. Nous sommes à même de nous demander si un tel système serait capable de remplir ce critère dans des circonstances de guerres contre-insurrectionnel dû à l'extrême complexité du champ de bataille. Dans de telles circonstances, la distinction entre les civiles et les combattants sera aussi un principe difficile à assurer : « even autonomous systems equipped with the most robust sensor packages may have difficulty fulfilling this requirement » (Thurnher, 2013). En fait, ce type d'armement pourrait difficilement remplir tous les critères nécessaires puisque la base d'une arme complètement automatisée est qu'elle doit posséder une qualité intrinsèquement humaine, soit le jugement : « it is clear that the development of software that would be capable of carrying out such qualitative judgements is not possible with current technology, and is unlikely to be possible in the foreseeable future »⁴. Bref, les pays devraient en principes être chargés de la révision de leur armement en employant la méthode qu'ils croiront la plus efficace. Il nous faut faire la remarque que la qualité de cette révision sera largement dépendante de l'engagement du pays en question pour

⁴ International Committee of the Red Cross (ICRC). *Report of the ICRC Expert Meeting on "Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects"*, 26-28 March 2014. Geneva: ICRC, 2014. Available at <https://www.icrc.org/eng/assets/files/2014/expert-meeting-autonomous-weapons-icrc-report-2014-05-09.pdf>, accessed 24 March 2015. Isaacson, Andy. "Are You Following a Bot?". *The Atlantic*, 2 April 2011. Available at <http://www.theatlantic.com/magazine/archive/2011/05/are-you-following-a-bot/308448/>, accessed 13 december 2015.


faire régner le droit international. De plus, cette incertitude en révèle une autre, soit le fait qu'il n'existe aucun standard international en matière d'évaluation de ce type d'arme⁵. Les pays qui développent ce type d'armes appliqueront donc leur propre standard pour respecter les lois humanitaires internationales.

Sans normes internationales pour réguler la prolifération des armes automatisées ou l'existence d'une agence chargée d'effectuer la révision légale de cet armement, le rôle de gardien du droit humanitaire international que l'on peut accorder à l'article 36 sera grandement limité. En fait, peu importe la façon avec laquelle les pays approcheront cet enjeu, il est indéniable que les mesures engendrées par l'article 36 des protocoles additionnels de la convention de Genève laisseront la place à une « prévention différentielle du risque ». Les limites imposées par l'article 36 seront alors très relatives. À l'heure actuelle, alors que plus de 87 pays se sont exprimés sur la question en admettant pour la plupart qu'il faut examiner les enjeux plus en profondeur⁶, seuls 2 pays, dont les États-Unis et la Grande-Bretagne, ont officiellement créé des politiques pour légiférer sur la question. La position des États-Unis est révélatrice quant à la direction empruntée : « The speaker stated that the policy was developed in order to reduce risks associated with autonomy in weapon systems and specifically it "establishes guidelines designed to minimize the probability and consequences of failures in autonomous and semiautonomous weapon systems that could lead to unintended engagements »⁷. À cet effet, il faut noter que notre intention n'est pas de juger des précautions prises par les États-Unis, mais de démontrer que le rôle de l'Article 36 dont il est question sera majoritairement d'inciter les pays à clarifier leur position sur les armes automatisées et de démontrer comment ils aborderont les incertitudes qui leurs sont rattachés. Comme l'ont fait les États-Unis en 2012 en légiférant sur la question, les pays adopteront (en fonction de leur engagement respectif) différents modèles pour encadrer le développement de ce type d'arme. Cette logique de prévention du risque laisse la place à une énorme marge de manœuvre en privilégiant un discours d'experts qui ne tiendra pas compte de plusieurs enjeux liés à ce type d'armes. La question du jugement mentionné précédemment sera abordée différemment dépendamment des groupes d'experts employés par les différents pays et les « filtres » imposés par les lois humanitaires internationales laisseront passer des armes potentiellement dangereuses sous couvert des différents degrés de risques privilégiés.

⁵ *Ibid*

⁶ Voir « Campaign to stop killer robot : Country policy positions », March 2015 : http://www.stopkillerrobots.org/wp-content/uploads/2015/03/KRC_CCWexperts_Countries_25Mar2015.pdf

⁷ International Committee of the Red Cross (ICRC). *Report of the ICRC Expert Meeting on "Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects"*, 26-28 March 2014. Geneva: ICRC, 2014. Available at <https://www.icrc.org/eng/assets/files/2014/expert-meeting-autonomous-weapons-icrc-report-2014-05-09.pdf>, accessed 24 March 2015. Isaacson, Andy. "Are You Following a Bot?". *The Atlantic*, 2 April 2011. Available at <http://www.theatlantic.com/magazine/archive/2011/05/are-you-following-a-bot/308448/>, accessed 13 december 2015.



Il faut aussi prendre en considération que plusieurs des réserves concernant le développement d'armes automatisées relèvent de principes moraux. La tenue d'un discours d'experts dans l'optique d'une prévention du risque occulte les enjeux moraux qui s'y rattachent en dénaturant la nature des enjeux. Au final, le rôle de l'article 36 sera, au mieux, de faire respecter les lois humanitaires internationales en limitant les dégâts que pourrait causer ces armes sans aucun principe de révision, et au pire, de n'avoir comme réelles conséquences qu'une multitude de prises de positions différentes sur les risques que les pays sont prêts à accepter pour développer ce type d'arme. Dans tous les cas, les arguments moraux sont écartés des débats en écartant la prohibition au profit d'une logique de prévention du risque.

Graduate Research Award Presentation 3

KIERAN ALKERTON

Master's

Munk School of Global Affairs

University of Toronto

Kieran Alkerton is a second year Master of Global Affairs student at the Munk School of Global Affairs. He is interested in pursuing a career working on a range of human development and human rights issues. He most recently worked with the Foundation for Education and Development in rural Thailand developing new programs for Burmese migrants living in Thailand. Kieran has a penchant for travel, having lived and worked as a tour guide and teacher in Québec City, Nicaragua, Guatemala, and Spain. At the Munk School, Kieran serves as a Mentor with the Global Ideas Institute, an associate editor with the Journal of International Law and International Relations, and the Director of Activities with the Student Association. Previously Kieran completed his undergraduate degree in Political Science and Classics from McMaster University in his home town of Hamilton, Ontario.

TOPIC: Space Security and Cyber Security: What are the common issues and challenges associated with cyber security and space security? What types of solutions could be offered to these challenges?

The Case for Cyber Security and Space Security as a Global Public Good

Introduction

Space security and cybersecurity are well-suited for comparison, both because of similar challenges to achieving international agreement and because of the actual connectivity between their infrastructures. Many states struggle to address the security risks inherent to both, and the unique nature of these risks makes conventional arms control treaties nearly impossible. The result is the emergence of an 'escalatory cycle' that catalyzes the militarization of both realms (Baylon, 2). Given the failure to establish a traditional security regime, a drastically different approach is needed to mitigate this militarization. At the state level, a number of scholars have suggested that cybersecurity can be considered a public good, defined as both non-rivalrous and non-excludable. This paper will seek to prove that treating international space and cybersecurity as a global public good could circumvent many of the challenges at the intersection of these security issues. The first part will discuss the public good characteristics of both realms, and suggest that the utility provided by their collective infrastructure can be conceptualized as a singular global public good referred to as digital security. The second will demonstrate how this approach can circumvent the collective action problems driving the militarization of the two realms. The final part will discuss the characteristics of a multilateral regime based on digital security as a global public good, and make recommendations for further research.

There is a growing body of scholarly literature which suggests that cybersecurity can and should be treated as a public good. Coyne and Leeson discuss the degree to which Internet security meets the criteria of a public good, namely whether it is non-rivalrous and non-excludable. First, they determine that the Internet is strongly non-rivalrous as “the value of each connection increases as the total number of connections increases” (Coyne and Leeson, 8). It is important to note that the positive externalities of the Internet as a whole are indispensable to the concept of Internet security as a public good. Without the good created by the multitude of contributions to the Internet its security is worth very little. Conversely, without cybersecurity the volume of users and the value of the Internet would arguably decline. Second, while the Internet and Internet security are excludable in the sense that access and security software both require payment, “there are positive spillover benefits in that those interacting with the uninfected user do not have to be concerned with virus infection from that user” (Coyne and Leeson, 8).

This concept of cybersecurity as a public good can be usefully expanded to the collective international security of space and cyberspace, and doing so arguably strengthens its public good characteristics. When applied at the international level, the positive externalities of the Internet and its security are significantly less excludable, since many state actors who do not contribute greatly to the infrastructure are nonetheless able to benefit from it. Through the international flow of information fostered by cyber networks, there are a number of other global utilities upon which populations around the world have grown to depend. These utilities share the same public good characteristics as international cybersecurity, and most interestingly, many of these are also critically connected to global outer space infrastructure. Space utilities such as the Global Positioning System and remote sensing satellites are used for “functions as diverse as weather forecasting, navigation, and search-and-rescue operations” (Space Security Index 2015, 13). These systems and the vast majority of outer space infrastructure depend on cyber networks, and “can be used by any actor equipped to receive the data they provide” (Space Security Index 2015, 13).

This collective of interconnected cyber and outer space infrastructures around the world can be reconceptualized as a new category that represents the global digital information infrastructure. It is a system that is made up of separate components that create a good that is larger than the sum of its parts. Digital security consists of the protection of this system, and it has strong global public good characteristics. States and their populations can benefit from its utilities without diminishing its value, and the barriers to inclusion are very low. Given these characteristics, a strong case can be made in favour of treating the security of this system as a global public good. Most importantly, a multilateral approach under this framework could circumvent many of the collective action problems facing space and cybersecurity and de-incentivize the continued escalatory cycle of militarization in these realms.

Part II: De-incentivizing militarization through the promotion of digital security as a public good

This section will discuss how promoting digital security as a global public good can mitigate the factors that are driving the militarization of outer and cyber space. It will focus on three important impediments to international cooperation: the definition of terms, monitoring and verification, and the low cost of militarization (Baylon, 2-3).

Definitions and terminology play an important in multilateral cooperation, and failure to reach consensus on the definition of terms has precluded negotiations on improving global cyber and space security from even beginning. The problem is largely political: the United States leads one camp, while China and Russia lead the other. In the realm of cybersecurity, the disagreement is centered around the Chinese and Russian desire to protect themselves from political instability caused by the free flow of information on the Internet (Baylon, 9). In space, the debate is over the inclusion of anti-satellite missiles in the category of 'space weapons' (Baylon, 10). The framework of digital security as a global public good would allow multilateral institutions to increase cooperation without wading into the political swamp created by these definitions. The maintenance of the systems that provide the vital global utilities discussed above would be the principle goal, and as such no mention of particular threats or weapons is required.

Dual-use technologies have complicated the monitoring and verification processes of many international security regimes. In both cyberspace and outer space, the line between military and civilian technologies is so blurry that it is nearly impossible to determine if a state is developing a military cyber or space program (Baylon, 10). This uncertainty decreases the likelihood of international cooperation, and makes traditional arms control treaties such as weapon bans incredibly impractical. The logic of the global public good, however, can mitigate the threat without having to single out and regulate the proliferation of any one kind of technology or knowledge. Instead, monitoring efforts could focus on the degree to which states maintain the integrity of the global digital infrastructure.

Lastly, the lack of incentive for multilateral cooperation on space and cyber security has been compounded by the low cost of militarization as an alternative to a negotiated agreement. In both realms it is financially and logistically easier to launch attacks than to defend against them (Baylon, 12). If the security of these realms was a global public good, however, the cost of launching an attack could be increased substantially and offensive strategies would no longer be the cheapest. Mulligan and Schneider describe this approach as a doctrine of deterrence through accountability, in which attacks on the infrastructure that provides the good are classified as crimes. States with little space and cyber infrastructure who originally had very little to lose will be de-incentivized from attacking. The states who own the infrastructure would have a lot to gain from cooperation, since it is their systems that would be protected as a public good.

A multilateral regime that treats digital security as a public good would operationalize the theory that intervention in the 'market' is required if adequate levels of security are to be maintained (Coyne and Leeson, 9). The provision of the good can be divided into two components: negative and positive. The negative component addresses the militarization of outer space and cyberspace, and its provision entails guaranteeing the absence of attacks. In this sense, an attack leading to the destruction of the global digital infrastructure would be akin to the destruction of the ozone layer through the use of chlorofluorocarbons. In the positive sense, the provision of digital security as a public good would consist of working towards ensuring that the benefits are distributed globally. For example, it would lay the framework for including digital infrastructure as a component of international development. However, ultimately these details exist on a spectrum, and the language can be restricted or expanded with a view to achieving international agreement.

Further research would engage more substantively with the collective action problems inherent to cyber and outer space security, in order to address potential criticisms of the global public good approach. It would also be useful to include case studies of existing multilateral and national regimes based on the provision and protection of public goods to generate useful recommendations for the implementation of the proposal.

WORKS CITED

Baylon, Caroline. "Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives", Chatham House, 2014.

Coyne, Christopher, and Peter Leeson. *Who protects cyberspace*. Global Prosperity Initiative Working Paper 37, Mercatus Center, George Mason University, 2004.

Mulligan, Deirdre K., and Fred B. Schneider. "Doctrine for cybersecurity", *Daedalus* 140.4 (2011): 70-92.

SPACESECURITY.ORG, Space Security Index 2015, Executive Summary. <http://spacesecurityindex.org/wp-content/uploads/2015/06/executive.summary.2015-electronic.pdf>. Date of Access: December 13, 2015.

Graduate Research Award Presentation 4

Daniel Golston

Master's

International Relations and Politics

University of Cambridge, Fitzwilliam College

Daniel Golston is currently pursuing a M.Phil in International Relations and Politics at the University of Cambridge in the United Kingdom. His course work focuses on international security, foreign policy analysis and public policy analysis. He will be writing his thesis on cybersecurity and international relations, with a focus on the rise of state-level acquisition of zero-day vulnerability software exploits and relevant implications for traditional conceptions of power in the international system. Additionally, Daniel is an Associate for The Policy Lab, a Boston-based think tank dedicated to improving the impact of public policy initiatives. He is also currently a volunteer consultant at the Cambridge Hub, a student-led group which offers consulting services to the local community, his specific project focuses on homelessness and encouraging better coordination between local charities, businesses and student groups. Before coming to Cambridge, Daniel spent 18 months at the United Nations Institute for Disarmament Research as a Project Assistant and Junior Researcher in the Emerging Security Threats Programme. Daniel holds a B.A. in International Relations from the University of British Columbia where he worked as an editor for the University's Journal of Political Science."

TOPIC: Space Security and Cyber Security: What are the common issues and challenges associated with cyber security and space security? What types of solutions could be offered to these challenges?

A REFOCUS ON NORMS: PURSUING CYBER AND OUTER SPACE STABILITY IN THE FACE OF SLOW REGULATORY PROCESSES

Every state on earth utilizes cyberspace and outer space (C&OS) to some extent. Concurrently, more states than ever are pursuing militarized capabilities in C&OS without elucidating national strategies or intentions.¹ Relevant multilateral regulatory initiatives are slowed by great power politics (between the United States, Russia and China) and the lack of a mutually-agreed lexicon. This has resulted in two crowded domains where technological innovation outstrips what little regulation is present,² widening the possibilities for misunderstanding and subsequent escalation into kinetic conflict. Therefore, the paramount challenge for states is how to continue in a cooperative direction despite increasing militarization and prevailing issues with regulation?³ To overcome this, states should refocus diplomatic energy away from overarching initiatives, and towards bi- and multilateral norm development.

1. THE ISSUES COMMON TO BOTH DOMAINS

Existing regulatory discussions suffer from a lack of a common lexicon, leaving states to determine subjective, *ad hoc* definitions. This issue hinders effective communication.⁴ For example, Western states commonly favour the term 'cyber security' while China and Russia

prefer ‘information security’.⁵ Not a minor technicality, this distinction represents divergent assumptions about the most fundamental nature of cyberspace; similar issues exist with terms such as ‘space weapon’⁶ and ‘cyber warfare’.⁷ Defining key concepts is a foundational requisite for comprehensive regulation, therefore a lack of common understanding is problematic.

Another pertinent issue is the increased militarization of C&OS. In part, this is driven by a widespread “lack or inadequacy of national policy documents” elucidating intent,⁸ and a general aura of mistrust,⁹ at least between the great powers.¹⁰ More states are pursuing militarized capabilities in C&OS to advance national security objectives,¹¹ which means assets in both domains become targets for attack,¹² prompting greater defensive militarization in response. States may also be inclined to pursue increased militarization in tandem with their growing utilization of C&OS, as a way to protect their investments.¹³ These phenomena have the power to undermine trust and stability and are not likely to subside in the short term. Combined, these issues beg the question: what is the best way forward?

2. THE SOLUTION: BI- AND MULTILATERAL NORM DEVELOPMENT

If states wish to continue reaping the benefits of a stable C&OS, they should refocus on solidifying bi-and multilateral norms of behaviour¹⁴ which derive from the confluence of national- and international-level interests.¹⁵ For states like Canada, an important national interest should be to secure the future, potential opportunities in C&OS. This interest is flexible, cooperative and conducive to the international-level interest of regulating both domains in pursuit of security and stability. Where interests align, i.e. on space debris mitigation¹⁶ or the protection of critical cyber infrastructure,¹⁷ norm development can continue to move the international community in a positive direction.

States should position themselves as “norm entrepreneurs” capable of rallying support for causes that benefit all parties involved,¹⁸ such as Canadian efforts against the weaponization of outer space.¹⁹ These efforts also provide states with agenda-setting power for future regulation by shaping “the dominant values [and] procedures”.²⁰ However, refocusing on norm development does not imply a rejection of regulatory initiatives; states should continue to be engaged albeit with the understanding that progress will be slow and deeply politicized.²¹

3. CONCLUSION

For the foreseeable future, states will continue militarizing their usage of C&OS. Despite the slow pace of regulation, it is incumbent upon states to continue to contribute towards stability through norm development in the interim. The recent success of the Russian initiative against the placement of weapons in outer space at the United Nations is commendable, however the persistent and predictable criticisms from the United States regarding the lack of mutual understanding of “operative terminology” epitomizes the issues highlighted in this article.²²

¹ Caroline Baylon. *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*. Publication. London: Chatham House, 2014: 8.

² Cesar Jaramillo argues that the Outer Space Treaty’s “precepts and underlying assumptions fall short of addressing the drastically changed reality of outer space activities today,” in: Cesar Jaramillo. “The multifaceted nature of space security challenges.” *Space Policy* 33 (2015): 63. In the cyber domain, there exists no comprehensive code of conduct.

³ In the outer space domain, such initiatives include the Chinese and Russian-proposed Treaty on the Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects, and the European Union-proposed International Code of Conduct for Outer Space Activities. In the cyber domain, this includes the Chinese, Russian, Tajik, and Uzbek-proposed International Code of Conduct for Information Security.

⁴ Baylon 9. Additionally, for the implications of a lack of definitions for key concepts, see presentations by: Tim Maurer, Aapo Cederberg, and Neno Malisevic at: Proceedings of UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict, United Nations Office at Geneva, Geneva. *United Nations Institute for Disarmament Research*, 2014. Web. & a presentation by: Nils Melzer at: Proceedings of UNIDIR Cyber Stability Seminar 2015: Regime Coherence, United Nations Office at Geneva, Geneva. *United Nations Institute for Disarmament Research*, 2015. Web.

⁵ Baylon 9.

⁶ Proc. of UNIDIR Space Security 2014 Conference The Evolving Space Security Regime: Implementation, Compliance, and New Initiatives, United Nations at Geneva, Geneva, *United Nations Institute for Disarmament Research*, 2014: 11.

⁷ Michael Robinson, Kevin Jones and Helge Janicke, 'Cyber warfare: Issues and challenges,' *Computer & Security* 49 (2015): 70-94.

⁸ For example: India "is increasingly dependent on space activities and has been seeking space-related arms largely as a deterrent against perceived threats," in: "An Analysis of Emerging Space Capabilities in Eurasia and Rising Security Tensions." *United Nations Institute for Disarmament Research*. 2014: 7.

⁹ Norms are defined as non-binding, non-formally codified, voluntary standards of proper and accepted behavior. The argument can be made that codes of conduct and legal treaties constitute norm development, as well. However for the purposes of this paper, norms are seen as the standards of behavior in place for example, at the time of establishing a code of conduct. They form the foundation for such codified processes and thus are distinct and precursory.

Definition derived in part from: Michael Krepon, "Norm Setting for Outer Space," *SpaceNews*. 8 December 2014. Web.

¹⁰ Jana Robinson. "Transparency and confidence-building measures for space security." *Space Policy* 27 (2011): 34.

¹¹ Baylon 8. This is also explored by Paul Meyer: "A 2012 survey by the UN Institute for Disarmament Research (UNIDIR) revealed that 114 states have a national cyber-security program, and 47 of these assign some role to the armed forces in carrying out that national program. Yet according to the UNIDIR research, only six states have published military cyber-security strategies, with varying degrees of specificity. While these findings point to a lack of transparency in cyber-security policies, they also suggest that a certain "militarization" of cyberspace is underway without much public debate on the matter," in: Paul Meyer. "Seizing the Diplomatic Initiative to Control Cyber Conflict." *The Washington Quarterly* 38:2 (2015): 48.

¹² In the space domain, mistrust was a prominent theme in the 2013 United Nations Group of Governmental Experts report on Transparency and Confidence-Building Measures in Outer Space Activities: "a proposed transparency and confidence-building measure should: [...] Reduce or even eliminate the causes of mistrust, misunderstanding, and miscalculation with regard to the activities and intentions of States," in: U.N. General Assembly, 68th Session, *Group of Governmental Experts report on Transparency and Confidence-Building Measures in Outer Space Activities* (A/68/189). 29 July 2013. (New York): 15.

¹³ As an illustrative example of mistrust between China and the United State in outer space, see: Brian Weeden, "An Opportunity to Use the Space Domain to Strengthen the U.S.-China Relationship." *National Bureau of Asian Research* 17 September 2015. As regards the cyber domain, in 2013 Karina Ibrahim suggested that the failure of the United States and Russia to secure a cyber security partnership stems from the history of mistrust "further exacerbated by the ongoing allegations of cyber-attacks and cyber-espionage," in: Karina Ibrahim, "From Arms Race to Cyber-Space: U.S.-Russian Relations and the Prospects of Cyber Warfare." *Center for Strategic and International Studies Rep's Blog*. 17 June 2013. Web. Additionally, in 2014, the United State Cyber Command refused to give up one important set of exploits used in offensive cyber capabilities, claiming that it would amount to "unilateral disarmament", one senior intelligence official stated that "the Chinese won't stop just because we do", in: Nicole Perlroth and David Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *The New York Times*. 13 July 2013. Web.

- ¹⁴ For example in the cyber domain, as of 2013, 41 states had explicitly acknowledged “some military planning or specific military organizations for cyber activities,” in: “The Cyber Index: International Security Trends and Realities.” *United Nations Institute for Disarmament Research*. 2013: 3.
- ¹⁵ Two recent and relevant events: China and Russia have tested anti-satellite missiles in October and November 2015, respectively. For more information, see: Bill Gertz, “Russia Flight Tests Anti-Satellite Missile,” *The Washington Free Beacon*. 2 December 2015. Web. Bill Gertz, “China Tests Anti-Satellite Missile,” *The Washington Free Beacon*. 9 November 2015. Web.
- ¹⁶ For example, Canada, along with the Czech Republic and Germany, maintains an online compendium of national and international space debris mitigation mechanisms which proliferates relevant information as part of norm development on space debris mitigation. Indeed, all space-faring nations can agree that space debris mitigation is in the national interest however only a handful engage in substantial cooperation on this matter, beyond what may be requested of them in bodies such as the Inter-Agency Space Debris Coordination Committee. To visit this compendium, see: <http://www.unoosa.org/oosa/en/ourwork/topics/space-debris/compendium.html>.
- ¹⁷ U.N. General Assembly, 65th Session. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)*. 30 July 2010. (New York): 8.
- ¹⁸ Martha Finnemore and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization* 52.4 (1998): 897.
- ¹⁹ Marius Grinius. “Statement by Canada in the CD on Tabling of Canada’s Working Paper on TCBMs for Space Security.” Conference on Disarmament. United Nations, Geneva. 26 March 2009. *Government of Canada*. Web.
- ²⁰ Peter Bachrach and Morton S. Baratz. “Decisions and Nondecisions: An Analytical Framework.” *The American Political Science Review* 57.3 (1963): 632.
- ²¹ Jaramillo 63.
- ²² Matthew Bodner, “UN Adopts Russian Initiative Restricting Space Weapons,” *DefenseNews*. 9 December 2015. Web.

WORKS CITED

- “An Analysis of Emerging Space Capabilities in Eurasia and Rising Security Tensions.” *United Nations Institute for Disarmament Research*. 2014. Web. 7 December 2015.
- “Conference on Disarmament Statement of the European Union on PAROS.” Conference on Disarmament. United Nations, Geneva. 19 March 2013. *European External Action Service*. Web. 7 December 2015.
- “The Cyber Index: International Security Trends and Realities.” *United Nations Institute for Disarmament Research*. 2013. Web. 2 December 2015.
- Backrach, Peter and Morton S. Baratz. “Decisions and Nondecisions: An Analytical Framework.” *The American Political Science Review* 57.3 (1963): 632-642.
- Baylon, Caroline. *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*. Publication. London: Chatham House, 2014. Web. 7 December 2015.
- Bodner, Matthew, “UN Adopts Russian Initiative Restricting Space Weapons,” *DefenseNews*. 9 December 2015. Web. 1 December 2015.
- Finnemore, Martha and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization* 52.4 (1998): 887-917.
- Gertz, Bill, “Russia Flight Tests Anti-Satellite Missile,” *The Washington Free Beacon*. 2 December 2015. Web. 8 December 2015.

- Gertz, Bill, "China Tests Anti-Satellite Missile," *The Washington Free Beacon*. 9 November 2015. Web. 8 December 2015.
- Grinius, Marius. "Statement by Canada in the CD on Tabling of Canada's Working Paper on TCBMs for Space Security." Conference on Disarmament. United Nations, Geneva. 26 March 2009. *Government of Canada*. Web. 7 December 2015.
- Jaramillo, Cesar. "The multifaceted nature of space security challenges." *Space Policy* 33 (2015): 63-66.
- Krepon, Michael, "Norm Setting for Outer Space," *SpaceNews*. 8 December 2014. Web. 9 December 2015.
- Meyer, Paul. "Seizing the Diplomatic Initiative to Control Cyber Conflict." *The Washington Quarterly* 38:2 (2015): 47-61.
- Perlroth, Nicole and David Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *The New York Times*. 13 July 2013. Web. 7 December 2015.
- Proceedings of UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict, United Nations Office at Geneva, Geneva. United Nations Institute for Disarmament Research, 2014. Web. 8 Dec. 2015.
- Proceedings of UNIDIR Cyber Stability Seminar 2015: Regime Coherence, United Nations Office at Geneva, Geneva. United Nations Institute for Disarmament Research, 2015. Web. 5 December 2015.
- Proceedings of UNIDIR Space Security 2014 Conference The Evolving Space Security Regime: Implementation, Compliance, and New Initiatives, United Nations at Geneva, Geneva, *United Nations Institute for Disarmament Research*, 2014. Web. 6 December 2015.
- Robinson, Jana. "Transparency and confidence-building measures for space security." *Space Policy* 27 (2011): 27-37.
- Robinson, Michael, Kevin Jones and Helge Janicke, 'Cyber warfare: Issues and challenges' *Computer & Security* 49 (2015): 70- 94.
- U.N. General Assembly, 68th Session, *Group of Governmental Experts report on Transparency and Confidence-Building Measures in Outer Space Activities* (A/68/189). 29 July 2013. (New York).
- U.N. General Assembly, 68th Session. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98*). 24 June 2013. (New York).
- U.N. General Assembly, 65th Session. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/65/201). 30 July 2010. (New York).
- Weeden, Brian, "An Opportunity to Use the Space Domain to Strengthen the U.S.-China Relationship." *National Bureau of Asian Research*, 17 September 2015. Web. 7 December 2015.

Keynote Address

Bruce G. Blair, Ph.D.

Co-Founder, Global Zero

and Research Scholar, Program on Science and Technology

Princeton University

“Reducing the Risks of Nuclear Weapons Use”

My longstanding interest in nuclear risk has been personal as well as professional, ever since I figured out how to circumvent the safeguards on nuclear-tipped missiles under my control in the 1970s. I and one other young launch officer could have illicitly fired up to 50 intercontinental rockets aimed at the Soviet Union, and China. We could have single-handedly destroyed their major cities, with the explosive equivalent of 4000 Hiroshima bombs. We actually could have done much worse by sending a launch order with valid codes to other units of the strategic nuclear forces, whose standing rule was to accept and execute a validated launch order regardless of its source. If a little birdie flew into a launch center wearing a neck band with a note that authenticated properly, you were under strict orders to launch your forces.

Later on, in 1977, the land-based missiles were locked up electro-mechanically. To fire them, the crews first had to unlock them, and this required a code that would be released to the crews by high-level nuclear command posts only in the event of war.

This case illustrates how U.S. safeguards against unauthorized launch became more stringent over time. Early in the Cold War, the top priority was to ensure that nukes could ‘always’ be used when directed. Ensuring that they could ‘never’ be used except when directed was a secondary priority. This balance between ‘always’ and ‘never’ trended toward an emphasis on ‘never’ in all of the major categories of nuclear risk.

Nevertheless, significant nuclear risks remain in the U.S. system, and even greater and growing risks exist in the nuclear postures of most of the eight other countries that possess nuclear weapons – risks of unauthorized launches, of accidental detonations, of mistaken launch caused by false warning of enemy attack, of crisis escalation that results in inadvertent or intentional use of nuclear weapons, and of weapons falling into the hands of terrorists through theft or capture.

My goal for this seminar is to highlight the trend lines of the basic risks of nuclear weapons use among the nine countries, and to identify some ways to reduce them.

Gaps remain in our knowledge, even for the relatively transparent U.S. system. New worrying deficiencies regularly crop up. Partly this reflects the emergence of new threats to nuclear command and control, such as cyber warfare, whose impact on safety and security has not yet been thoroughly analyzed. Often it simply reflects discoveries of previously overlooked problems.

For example, in the mid-1990s I advised an independent commission looking into possible scenarios in which U.S. nuclear forces might be used without authorization. Scores of scenarios were uncovered. One involved an electronic back door into the nuclear communications network. This early discovery anticipated the current concern with cyber intrusion into these networks. It also identified a serious deficiency in Trident submarine safeguards that led to the installation of a major new safeguard. (The captain's fire control key was placed inside of a safe whose unlock combination would be sent as part of the launch order.) These were old problems that only surfaced through independent review. This happens time and time again. You never really get to the bottom of things.

These gaps and uncertainties make it hard for any of the nine countries with nuclear weapons to defend the claim that their deterrent value outweighs the myriad risks of their use. I would further argue that the risks are far greater than generally believed, they are growing in some areas, and remedies are urgently needed.

The bottom line is none of the nine nuke nations are anywhere close to "never", to zero risk. All of them prepare for nuclear war, for ensuring that their nuclear forces can 'always' be used if called upon, and in preparing for nuclear war they risk causing it in some fashion or another.

I'll begin with the United States and Russia and weave the situation in other countries into the story.

The underlying cause of quite a few of the dangers in the U.S.-Russia case is the vulnerability of their nuclear chains of command. As I tried to prove in my book ("Strategic Command and Control"), a few tens of weapons could decapitate their nuclear leadership and sever the communications links used to send the "go-code" to strategic bombers, submarines, and land-based missiles.

To work around this vulnerability during the Cold War, the U.S. and Russia did several risky things that cast long shadows on the present.

First, all U.S. presidents from Eisenhower through Reagan pre-delegated their launch authority to multiple military commanders, each of whom obtained all the authorizing and unlocking codes needed to order a full-scale U.S. strategic attack. We're talking about upwards of a dozen senior commanders. It's easy to imagine scenarios in which a communications outage of even short duration would have resulted in an abrupt and irretrievable assumption of launch authority by one or more of these generals.

This pre-delegation was rolled back at the end of the Cold War but it remains alive in organizational culture, and the essential codes remain widely distributed within the military command system.

Soviet leaders by contrast distrusted their military and eschewed pre-delegation. Top-down centralized control was the core value of their political culture, going back to the Czars. The Soviets therefore invested huge sums in building underground command posts to protect top leaders, they infiltrated KGB and political officers into their nuclear chain of command from top to bottom, they installed sophisticated locks on all their strategic weapons at an early stage of the Cold War and held the unlocking codes at the highest levels, and they directly linked the top-level command posts to the missile launch equipment in the field so that they could bypass humans down the chain. They even went so far as to build an elaborate launch apparatus akin

to the “doomsday machine” in Dr. Strangelove to ensure semi-automatic nuclear retaliation in the event of a U.S. strike that incapacitated the top leadership.

But as the Moscow coup of 1991 demonstrated, when a country’s social and political contract collapses it can bring down with it the entire edifice of safeguards. In this case the coup plotters including the head of the KGB and the Defense Minister and other key officials, who became exhausted and inebriated in some cases, simply seized the nuclear reins from Gorbachev. A few years later an alcoholic named Yeltsin had his fingers on the nuclear button.

The standard assumption of rational actors at the apex of nuclear command at all times does not hold up so well, even in the U.S. case. I was on alert in a launch bunker during the 1973 Arab-Israeli War when an order came down directing us to move to a higher state of nuclear alert, retrieve our launch keys and codes from our safe, and strap into our chairs to brace for imminent nuclear explosions. Nixon was president at the time, but he was not in charge that night. He had retired to his quarters, reportedly inebriated, before Henry Kissinger and others ordered the alert.

In contrast to the Soviet penchant for locking up their strategic nukes, the U.S. delayed introducing locking devices requiring input from higher authority to fire the forces. The individual commanders possessed the technical ability to fire their weapons throughout most or all of the Cold War: until 1970 for bomber crews, 1977 for land-based Minuteman crews, and 1997 for submarine crews. These devices were and are far from foolproof, however.

By the 1970s and 80s, both sides adopted an accident-prone tactic known as launch on warning in order to ensure that their strategic forces could be fired before incoming warheads arrived. Given the 12- to 30-minute flight times of attacking missiles, nuclear decision-making – from warning to decision to action – became extremely rushed, emotionally charged, and pro-forma, driven by checklists. I describe it as the rote enactment of a prepared script. In some scenarios, after only a 3-minute assessment of early warning data, the U.S. president receives a 30-second briefing on his nuclear response options and their consequences. He then has a few minutes – 12 at most – to choose one.

Then a short launch order would be transmitted to launch crews. How short? It’s the length of a tweet. The crews in turn transmit a short stream of computer signals that immediately ignite the rocket engines of many hundred of land-based missiles. For the U.S., this takes 1 minute. I personally practiced it hundreds of times. We were called Minutemen. U.S. submarine crews can fire their missiles in 12 minutes.

Our heavy reliance on launch on warning means that the standard paradigm of stable mutual deterrence based on second-strike retaliation after absorbing a massive attack was an intellectual construct without operational meaning. A former four-star commander (Gen. George Lee Butler) of U.S. strategic forces explains:

“Our policy was premised on being able to accept the first wave of attacks.....Yet at the operational level it was never accepted....They [nuclear planners] built a construct that powerfully biased the president’s decision process toward launch before the arrival of the first enemy warhead ... a move in practice to a system structured to drive the president invariably toward a decision to launch under attack...”

Nuclear planners rigged the war plan to make launch on warning or preemption absolutely essential to achieving the plan's war aims. They effectively stripped presidents of any ability to ride out an attack before deciding how to respond. They also rigged the plan to ensure that the entire enemy target base including cities would be destroyed in the first salvo even if presidents tried to spare cities. And throughout the Cold War they did not allow any civilian experts to inspect the president's nuclear briefcase (the "football") carried by his military aide. Civilian officials were thus unable to ensure that the president's emergency response options in that briefcase conformed to the extant strategic war plan and to the nuclear employment guidance he issued in peacetime.

U.S. presidents went along with this, albeit reluctantly. They all acquiesced to the imperative of making a quick decision to fire on warning. Reagan (in his memoirs) complained about having only "Six minutes to decide how to respond to a blip on a radar scope and decide whether to release Armageddon!" Although admitting it was an accident prone policy, top security advisors such as Henry Kissinger and Brent Scowcroft argued in a top secret meeting that "It is not to our disadvantage if we appear irrational to the Soviets in this regard."

Well, this irrational posture remains intact today. Our nuclear command system and forces practice it several times a week. So do the Russians.

And believe it or not, Russia shortened the launch time even more. Today, top military command posts in the Moscow area can directly fire by remote control rockets in silos and on trucks as far away as Siberia in only 20 seconds.

Common sense tells us this is risky. Early warning teams in the U.S. receive sensor data at least once a day that requires them to urgently assess whether a nuclear attack is underway or the alarm is false. Once or twice a week they need to take a second close look, and once in a blue moon the attack looks real enough to bring them to the brink of launch on warning. The U.S. and Russia have come THIS close to disaster on several occasions involving false alarms. On one occasion, national security advisor Zbigniew Brzezinski was seconds away from waking President Carter in the middle of the night to inform him that the Soviets had launched an all-out nuclear attack and that he (Carter) would have to choose a retaliatory option without delay.

In the context of deteriorating relations that produce a crisis between them in future, the risk of mistaken launch may be even higher than it was during the Cold War because of the decrepit state of Russia's early warning network. Due to the total collapse of Russia's satellite early warning network, Russia's decision time for launch on warning has decreased to 2 to 4 minutes.

During a crisis, the pendulum swings back toward "always" and the pre-disposition of leaders to believe missile attack warning would of course be heightened. I have shown (in "The Logic of Accidental Nuclear War"), using Bayesian statistics, that a pre-disposed mind would rationally become convinced of an attack after only one or two cycles of positive attack indications from early warning sensors. (By positive I mean the sensors are reporting missiles launches whether or not the reports are correct.) This is a mistaken launch waiting to happen.

It's a risk that is relevant to other countries as well. Many of them are following in the footsteps of the U.S. and Russia in diversifying, dispersing, and forward deploying nuclear forces on ever higher states of alert. Let me run down the highlights.

For fifty years China has been a model of nuclear restraint. Almost all of its nuclear weapons in its modest arsenal sit at a single storage complex. Transportation and uploading to missiles and warplanes would take days to weeks. Control is highly centralized and reinforced by modern safeguards. In peacetime China thus runs a minimal risk of nuclear accidents, mistaken or unauthorized launches, or weapons falling into the hands of terrorists during transportation.

This restraint appears to be ending. Its nuclear command – the 2nd artillery – wants to put forces on higher alert and send them out on patrol on land and sea armed with warheads. It also wants the President (Xi Jinping) outfitted with a nuclear suitcase in order to expedite launch authorization. China will deploy its first strategic submarine within the next few months and it is expected to patrol armed with nuclear warheads. China may also begin outfitting some of its mobile strategic missiles on land with warheads. China also is developing an early warning satellite network that could support an option to launch on warning.

Like China, India is shifting its priority from ‘never’ to ‘always’. Today, in peacetime its nuclear forces are completely off alert. All warheads are kept disassembled under the custody of non-military departments. It would take days to weeks to mate them to delivery vehicles in the field. Once alerted in a crisis, India aims to poise them for launch within 30 minutes after receiving the order.

But like China, India also is going to increase its day-to-day readiness. Its first strategic submarine is scheduled for commissioning this year, and it is likely to be armed with nuclear weapons during peacetime patrols. India’s nuclear establishment is pressing hard for India to prepare its weapons and the command system for rapid operations in peacetime, crisis, or war. Prime Minister Modi has thus been equipped with a nuclear suitcase linked to dedicated communications circuits to expedite launch authorization.

Pakistan is in a league by itself in terms of nuclear risks. Pakistan has the fastest growing arsenal in the world and may well overtake China for third place before long. Although it currently keeps its nuclear warheads disassembled in peacetime, it is moving steadily toward a posture requiring early dispersal and early first use of its nuclear forces under more decentralized control during a crisis with India.

There are indications of jihadist sympathies within the military. With possible help from insiders, the terrorist capture and use of the weapons against India or Pakistan itself is a grave threat to South Asian security today. And the social fabric of the Pakistani state is in tatters. If it disintegrates some day, the safeguards against nuclear weapons falling into the hands of terrorists would likely collapse.

North Korea is weaponizing. It’s reportedly making headway in miniaturizing warheads to fit atop its missiles, but the missiles already have ample space in their nosecones to carry crude fission bombs to targets as far away as Japan. If and when this arming occurs, with an unpredictable leader’s finger on the button (Kim Jong Uen), a nuclear disaster will be waiting to happen in Northeast Asia.

U.K. and France. Both keep a single submarine on low-level alert at sea at all times.

Finally, Israel. Its nuclear status is opaque but it appears to be acquiring the capability to project nuclear threats on shorter notice than in the past. While its current arsenal is on a low level of alert in peacetime, Israel is reportedly deploying, into the Persian Gulf, strategic submarines

capable of launching nuclear cruise missiles. Depending on evolving threats in the region – particularly Iran’s nuclear program – Israel may establish regular nuclear-armed sea patrols.

Most of the newer nuclear weapons states appear to be decades behind the United States in terms of safety and safeguards – lagging in areas like one-point safety for warheads, insensitive high explosives, fire resistant plutonium pits, and modern locking devices.¹ After experiencing over one thousand incidents of varying degrees of severity during the growing pain years from 1950 to 1968 and many accidents that came very close to nuclear detonations (some on American soil), the U.S. has come a long way toward the ‘never’ end of the spectrum by designing and extensively testing weapons with these safety features. Other countries with a less advanced safety culture, with far fewer resources, few tests under their belt, and lacking the technological sophistication of the U.S. will likely run even higher risks of an accidental or unauthorized nuclear detonation during their growing pain years. These risks will only grow as they increase the readiness and operational tempo of their weapons.

Nor can the U.S. rest on its laurels. Six nuclear cruise missiles were loaded by mistake onto a U.S. strategic bomber and flown across the country in 2007. For more than a day, no one knew the payload was nuclear, no one knew the nukes went missing, and no one guarded them. More recently, we learned that launch officers often deliberately violate nuclear weapons safety rules, compromise the launch codes, and cheat on proficiency exams. Between 2009 and 2013 there were nearly 1,500 incidents involving Air Force nuclear weapons alone.

Russia’s nuclear risks are more complex and severe. Just three years ago a Russian sub caught fire in dry dock with a full complement of nuclear-tipped ballistic missiles onboard. Russia has far more nukes in transit at any time than any other country, and transportation is the Achilles Heel of nuke security. Nuclear materials security is subpar. There is a nuclear materials black market and dozens of cases of weapons-grade smuggling have surfaced. With 2,000 Russian Chechens fighting in Syria (for ISIL), Russia faces a growing threat of terrorism, perhaps nuclear terrorism, as fighters return.

A new factor in the risk equation is that nuclear command-control-communications and early warning networks may be vulnerable to cyber infiltration. Early warning data may be corrupted, or the actual launch circuits might be penetrated. Questions abound – could unauthorized actors – state or non-state – spoof early warning networks into reporting spurious attack indications that trigger a mistaken launch? Could hackers breach the firewalls, the air gaps, and transmit launch orders to launch crews or even to the weapons themselves? What if an insider colluded with outsiders to provide access and passwords to the launch circuits?

¹ Historically, the vast majority of serious nuclear accidents have involved crashes of nuclear-armed aircraft. Of the seven basic warhead types in the U.S. stockpile, all but one (the W-88 sub warhead; double-check on the W-76) have insensitive high explosives, meaning that they can withstand impacts of up to 1,500 feet per second as opposed to conventional high explosives which will detonate at only 100 feet per second. One-point safe means that a single-point detonation initiated anywhere on the warhead – such as might occur during a bomber crash – has a probability of no greater than one in a million of producing a nuclear yield in excess of four pounds of TNT equivalent. Fire resistant pits are designed to provide molten plutonium containment against the ~1000 degree C temperatures of an aircraft fuel fire that lasts for several hours. Several U.S. warheads (W-76; -80; -88) lack FRPs.

Contrary to popular belief, nuclear networks are not hermetically sealed. I mentioned earlier the discovery of an electronic backdoor that offered outsiders a way to get inside the U.S. naval broadcast network. They could have actually seized and operated remotely the main radio station used to transmit launch orders to subs in the Atlantic Ocean. The Navy took this threat so seriously that it completely revamped the procedures for validating launch orders, so that an order received out of the blue in peacetime would not be accepted as valid until it was verified by a second independent source.

In 2010, underground missile crews lost contact for an hour with a large field of Minuteman missiles in Wyoming. Soon after contact was lost, the supposedly fire-walled control network for these missiles was automatically opened. After a few minutes a timer expired and activated a radio antenna at each of the missile silos to receive commands from airborne launch centers. This gave outsiders a potential pathway for injecting the target, arm, and launch signals needed to fire the missiles. (The Air Force was initially panicked over the prospect that the field had been cyber attacked, and President Obama personally followed the investigation. Investigators determined the cause to be improper maintenance on a circuit board inside one of the squadron's launch control centers.)

Recent reviews of such vulnerabilities have left many unanswered questions. Given our poor comprehension of this cyber threat, it seems imprudent in the extreme to keep U.S. and Russian nuclear missiles on quick-launch alert, ready to fly as soon as they receive a short stream of computer signals.

Let me wind down with a discussion of crisis escalation resulting from brinksmanship and inadvertence. Preventing the use of nukes is supposed to be the job of a psychological construct known as 'deterrence', but deterrence can become an extreme sport during a confrontation, a game of taking and manipulating existential risk, morphing into games of chicken, bluff, coercion and blackmail. The basic idea is to instill fear in an adversary's mind that events could spin out of control and result in a nuclear war. Nuclear risk grows as the pendulum swings from "never" to "always" and safeguards are shed.

The last time the U.S. brandished nukes wholesale for this purpose was 1973 when Kissinger and team raised the global nuclear alert level. The aim was to warn Soviet leaders they had better back down or else face an escalating risk of nuclear war, driven not so much by premeditation as by inadvertence.

Russia's sounding of nuclear warnings over the Ukraine imbroglio is reminiscent of this Cold-War brinksmanship. The crisis is far from matching Cold War tensions, but there are risk-takers in the game, and we are witnessing the early stages of a spiral of action-reaction cycles along with dangerous unintended consequences.

Close encounters between Russian and Western military aircraft have spiked. NATO fighter planes have made many hundreds of intercepts of Russian warplanes over the past year. Russian warplanes have stepped up provocative overflights of foreign airspace, and also are engaged in muscular interdiction. For instance, a U.S. spy plane was forced to flee into Swedish airspace to escape harassment by Russian fighters.

At some point in a crisis these interactions multiply and become self-reinforcing, and begin to spin out of control and into what the strategist Tom Schelling calls "the threat that leaves something to chance".

A good illustration of this crisis dynamic is cycle of action-reaction evident in the Ukraine crisis. In order to reassure U.S. NATO allies in Eastern Europe, we have been flying U.S. strategic bombers to the area, (*sans* nuclear warheads, but the Russians do not know this for certain), sometimes in provocative formations. Russia countered with actions and threats involving nuclear-capable missiles (e.g., Iskanders). We also began deploying Aegis destroyers to the Black Sea to reassure allies like Romania. As it turns out, these ships carry a substantial arsenal of cruise missiles armed with conventional warheads, whose 1,000 mile range allows them to reach all the way to Moscow. By my calculations (my conventional “lethality” estimates), these stealthy weapons could strike without warning and destroy all but the hardest military targets. They could destroy the Kremlin without warning. Moreover the Russians cannot be 100 percent certain that the missiles are not nuclear-tipped.

That they may pose a decapitation threat probably underlies Russia’s harassment of the destroyers with fighter aircraft and its recent deployment of a fleet of attack submarines to the Black Sea. And in a further escalating response, NATO’s top naval commander has proposed deploying U.S. anti-submarine aircraft to new bases in the region to counter the Russian subs which now threaten our destroyers which now threaten Moscow.

At some point one side or the other may blink and back off, or maybe not. Tensions could continue to rise until the crisis escalates by intention or inadvertence to the threshold of nuclear use. In the case of Russia, this threshold is low. Russia’s strategy in Europe was devised by President Putin himself in the year 2000 in response to NATO’s bombing of the Balkans. The strategy is called “de-escalatory escalation”, which unleashes tens to hundreds of nuclear weapons in a first strike meant to shock an adversary into paralysis. And so it might, or it might just escalate into a nuclear exchange.


Even stronger escalatory updrafts would afflict the other nuclear countries in a confrontation, particularly Pakistan and India whose propensities toward escalating all the way are acute.

I am going to wind down this overview with several key conclusions before ticking off a set of recommendations for reducing nuclear risks. One, the Cold War was far more fraught with risk, and unstable, than the paradigm of mutual deterrence claimed it to be. Two, nuclear weapons escaped the control of the democratic process in the United States. Three, although some major risks have subsided in the case of the original five nuclear powers, other major risks persist, including the slippery and steep slope of crisis escalation. Four, the newest members of the nuclear club are running a multitude of growing risks. Pakistan in particular is a nuclear explosion waiting to happen. And five, given all this risk-taking, and given that deterrence itself is nothing more or less than the manipulation of nuclear risk, we cannot reasonably expect nuclear weapons never to be used. We are closer to “always” than “never”. We can reasonably expect to witness the use of nuclear weapons in our lifetime, somewhere in the world, unless we manage to eliminate them entirely during our lifetime.

Global Zero will not happen overnight. Meanwhile, the following seven measures would help move the dial further away from ‘always’ toward ‘never’:

One. The United States and Russia could agree to eliminate launch on warning from their strategy. They should immediately cease conducting exercises that involve launching strategic missiles on the basis of data from early warning sensors.

Two. They could agree to begin taking their strategic missile forces off of hair-trigger, by adopting physical measures such as downloading warheads to storage that extend the time



required to launch from the current period of minutes to a period of days. Beginning with an immediate 20 percent reduction in the size of their missile forces on high alert, the United States and Russia should verifiably stand down all their forces in phases over the next ten years.

Three. All the nuclear weapons countries could agree to refrain from putting any nuclear forces on high alert except under tightly controlled conditions. This agreement would sharply limit the scope and timing of any re-alerting undertaken for training, exercising, or national security emergencies, and would require pre-notification of such activities.

Four. The U.S. and Russia could work with other nuclear establishments to share knowledge, best practices, and technologies in the area of safety and security.

Five. The U.S. and Russia, perhaps with China, could lead an effort to ban cyberwarfare aimed at nuclear command, control, communications and early warning networks. These networks should be strictly off limits to cyber attack.

Six. Nuclear safeguards could be designed on the assumption of insider collusion involving two or more people working with outsiders, replacing the prevailing threat model that assumes only a single insider working with outsiders.

And Seven. Confidence-building measures agreed to through military-to-military dialogue could help reduce the risk that geopolitical tensions around the world could escalate by design or inadvertence to the nuclear threshold. I defer to my brilliant international relations colleagues at the Wilson school for deeper solutions to these deep structural security dilemmas.

Thank you.

Expert Review Panel

Andrea Berger is the Deputy Director of the Proliferation and Nuclear Policy programme at RUSI and a Senior Research Fellow. Her research interests include non-proliferation, arms control, sanctions policy and Korean Peninsula security issues. Andrea is also director for the UK Project on Nuclear Issues (UK PONI).

Prior to joining RUSI, Andrea worked in non-proliferation research and analysis at the International Centre for Security Analysis. She has also worked for the government of Canada in a number of analytical capacities, lastly in the Department of Foreign Affairs, Trade and Development.

Andrea holds an MA in International Peace and Security from the Department of War Studies at King's College London, a BA in Political Science from Carleton University in Ottawa, as well as a certificate in Nuclear Safeguards and Non-Proliferation from the European Safeguards Research and Development Association.

Christopher Penny is Assistant Professor of International Law at the Norman Paterson School of International Affairs, Carleton University. Prior to joining the full-time faculty, he taught as a sessional lecturer at NPSIA as well as at the University of Ottawa Faculty of Law (where he also coordinated the International Law program). Professor Penny is a member in good standing of the Law Society of Upper Canada. In addition to his position at NPSIA, he is also a reserve legal officer (Army Lieutenant-Colonel) with the Canadian Forces, serving in the Directorate of International and Operational Law in the Office of the Judge Advocate General.

In addition to his academic work, Professor Penny also has substantial practical experience with the development and application of international law in this field. He has participated as a member of the Canadian government delegation to numerous multilateral treaty negotiations, both within and outside of the United Nations framework, and has also provided legal advice in operational military environments relating to NATO operations in Afghanistan and Libya.

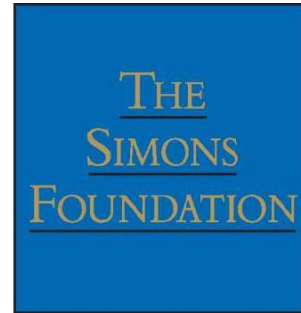
Cindy Vestergaard is a Nonresident Fellow with the Managing Across Boundaries Initiative and a senior researcher at the Danish Institute for International Studies (DIIS) in Copenhagen, Denmark. Her current research focuses on the global governance of natural uranium, including major suppliers (Australia, Canada, Kazakhstan) and the debates surrounding potential emerging suppliers (such as Greenland and Tanzania) and consumers (i.e. India). Vestergaard's research portfolio also includes chemical weapons disarmament, biosecurity and import/export controls.

Previous to joining DIIS, Vestergaard worked on non-proliferation, arms control and disarmament policy and programming at Canada's Department of Foreign Affairs and International Trade. Positions, among others, included Senior Policy Advisor, Global Partnership Program; Senior Policy Advisor, Foreign Intelligence Division; and Political Officer at Canada's Mission to Hungary and Slovenia.

Annex 1

ISROP
INTERNATIONAL
SECURITY RESEARCH
AND OUTREACH
PROGRAMME

PRISI
PROGRAMME
DE RECHERCHE
ET D'INFORMATION
DANS LE DOMAINE
DE LA SÉCURITÉ
INTERNATIONALE



Graduate Research Awards for Disarmament, Arms Control and Non-Proliferation 2015-2016 competition

February 26th 2016
10:00- 12:00pm
Room A9-26

9:50 Coffee/ Refreshments

10:00 Opening Remarks

Martin Larose – Director, Non-Proliferation and Disarmament Division

Remarks by Dr. Jennifer Allen Simons, President of The Simons Foundation

10:25 Presentation on Masters Questions + (Q&A)

1. *What role could Article 36 of the Additional Protocol (I) of the Geneva Conventions and the requirement for weapon reviews play in addressing new and emerging technologies, such as lethal autonomous weapons systems?*
 - Jenny Yang – University of Cambridge
 - Sacha Lavoie-Guilini – University of Ottawa
2. *Space Security and Cyber Security: What are the common issues and challenges associated with cyber security and space security? What types of solutions could be offered to these challenges?*
 - Kieran Alkerton – University of Toronto
 - Daniel Golson – University of Cambridge

11:45 Expert Briefing – Dr. Bruce Blair, Simons Foundation + (Q&A)

12:00 Closing Remarks and awards to GRA Debate Winners

Dr. Jennifer Allen Simons, President, The Simons Foundation (presentation of awards)

Martin Larose – Director, Non-Proliferation and Disarmament Division

12:15 Lunch

Annex II

GRADUATE RESEARCH AWARDS ***for Disarmament, Arms Control and Non-Proliferation*** **2015-2016**

\$5,000

Competition Details

Graduate Research Awards for Disarmament, Arms Control and Non-Proliferation are offered by The Simons Foundation and the International Security Research and Outreach Programme (ISROP) of Foreign Affairs, Trade and Development Canada (DFATD).

The 2015-2016 competition has been revised to simplify the application process and increase the value of the cash awards. A total of four awards of CAD\$5,000 are available to Canadian Master's and/or Doctoral candidates to support the research and writing of an academic paper responding to a specific Non-Proliferation, Arms Control and Disarmament (NACD) topic. Awards also include travel support to Ottawa where successful candidates will present their completed papers during a special event at DFATD Headquarters on February 26, 2016.

Deadline for applications:	December 14, 2015
Selection of four award recipients:	January 18, 2016
Presentations at DFATD in Ottawa:	February 26, 2016

HOW TO APPLY:

Applications should be sent to Elaine Hynes at The Simons Foundation by email to:

ehynes@thesimonsfoundation.ca by the close of business (PST) on December 14, 2015.

Your application must include:

- Your resume, including proof of citizenship status.
- A complete, official transcript of your grades (electronic copies of official transcripts are acceptable).
- An academic paper (1,500 words) responding to one of the specific Non-Proliferation, Arms Control and Disarmament topics shown below.

ELIGIBILITY:

The competition is open to Canadian citizens and Canadian permanent residents/landed immigrants currently enrolled in a graduate programme at a university in Canada. Previous recipients of a Graduate Research Award are not eligible in order to expand the community of Canadian scholars working on non-proliferation, arms control and disarmament (NACD) issues.

SELECTION PROCESS:

Applications will be reviewed by an Expert Review Panel made up of three experts and academics working in this field who will recommend four award winners for final approval by representatives of The Simons Foundation and ISROP. Successful candidates will be notified on January 18, 2016.

PRESENTATIONS AT DFATD:

Award winners will be invited to present their papers at a special event hosted by DFATD at DFATD Headquarters in Ottawa on February 26, 2016 and will be asked to produce a PowerPoint deck for their presentation. The cash awards will also be presented at the GRA event in Ottawa and a report, including the papers presented, will be published online by The Simons Foundation. ***Please note that attendance at the GRA event in Ottawa is a mandatory requirement of the award.*** Approved travel, accommodation and meal expenses will be provided by The Simons Foundation.

TOPICS for 2015-2016

Master's Candidates:

1. What role could Article 36 of the Additional Protocol (I) of the Geneva Conventions and the requirement for weapon reviews play in addressing new and emerging technologies, such as lethal autonomous weapons systems?
2. Space Security and Cyber Security: What are the common issues and challenges associated with cyber security and space security? What types of solutions could be offered to these challenges?

Doctoral Candidates:

3. Improving Canada's counter-proliferation architecture: what policy proposals/legislative amendments could be developed to close Canada's remaining counter-proliferation gaps?
4. Which approach is more likely to achieve a world without nuclear weapons – the immediate negotiation of a Nuclear Weapons Convention *OR* pursuing a step-by-step process to negotiate and implement complementary legal instruments and political agreements, like the NPT, the CTBT, an FMCT, etc.?

Suggested reading lists for each topic are available upon request. To receive a copy, please contact Elaine Hynes at The Simons Foundation by email to ehynes@thesimonsfoundation.ca or at telephone number 778-782-7779.

The primary objective of the Graduate Research Awards is to enhance Canadian graduate level scholarship on disarmament, arms control and non-proliferation issues.

BOURSES DE RECHERCHE AUX CYCLES SUPÉRIEURS (BRCS)
pour le désarmement, le contrôle des armements et la non-prolifération
2015-2016

5,000\$

Détails de l'appel de candidatures

Les ***Bourses de recherche aux cycles supérieurs pour le désarmement, le contrôle des armements et la non-prolifération 2015-2016*** sont décernées par la Simons Foundation et le Programme de recherche et d'information dans le domaine de la sécurité internationale (PRISI) du Ministère des Affaires étrangères et du Commerce international (MAECD).

La compétition 2015-2016 a été révisé afin de simplifier le processus de demande et d'augmenter les bourses à 5 000 \$CAN. Les bourses seront décernées à des étudiants canadiens à la maîtrise ou au doctorat pour leur permettre d'effectuer de la recherche et produire un document académique sur un sujet ci-dessous. Les bourses comprennent les frais de déplacement pour venir à Ottawa (transport intérieur, hébergement et repas), où les candidats sélectionnés seront invités à présenter à l'occasion d'une rencontre spéciale qui se tiendra au MAECD le 26 février 2016.

Date limite pour l'appel de candidatures :	le 14 décembre 2015
Sélection des quatre boursiers:	le 18 janvier 2016
Les présentations au MAECD:	le 26 février 2016

COMMENT POSER SA CANDIDATURE

Vous devez adresser votre demande de participation à M^{me} Elaine Hynes de la Simons Foundation par courrier électronique (ehynes@thesimonsfoundation.ca) d'ici le 14 décembre, avant la fin des heures de bureau (HNP).

Les dossiers de candidature doivent comprendre :

- Un curriculum vitae, y compris une preuve de citoyenneté;
- Un relevé de notes officiel et complet (des copies électroniques des relevés de notes officiels sont acceptables)
- Un échantillon de texte de 1 500 mots sur un des questions sur la non-prolifération, au contrôle des armements et au désarmement indiqué ci-dessous;

ADMISSIBILITÉ

Les citoyens canadiens ainsi que les résidents permanents/immigrants reçus peuvent poser leur candidature, y compris les diplômés canadiens qui poursuivent actuellement des études à l'étranger. Les anciens boursiers du programme BRCS peuvent aussi poser leur candidature, mais la priorité sera accordée aux étudiants qui n'y ont pas encore participé.

PROCESSUS DE SÉLECTION

Les dossiers des candidates seront examinés par un comité d'experts composé de trois experts et des universitaires travaillant dans ce domaine, qui vous recommandera quatre lauréats pour approbation finale par les représentants de la Fondation Simons et PRISI. Les candidats retenus seront avisés le 18 janvier 2016.

PRÉSENTATION

Les lauréats des bourses seront invités à présenter (avec PowerPoint) leurs énoncés, le 26 février 2016 à Ottawa, sous l'égide du MAECD. La Simons Foundation diffusera en ligne un compte rendu de ces discussions.

Prière de noter que les boursiers sélectionnés doivent obligatoirement participer aux BRCS. Les frais de déplacement, l'hébergement et les repas seront à la charge du PRISI, conformément aux directives applicables du Conseil du Trésor du gouvernement du Canada et, au besoin, grâce à une aide financière supplémentaire de la Simons Foundation.

BRES 2015-2016 : Sujets proposés pour les étudiants à la maîtrise et au doctorat

Candidate avec des Maîtrises :

1. Quel rôle l'article 36 de la Protocole additionnel (I) aux Conventions de Genève et l'exigence relative aux examens sur les armes pourraient-ils jouer dans la prise de mesures à l'égard des technologies nouvelles et émergentes, comme les systèmes d'armes létales autonomes?
2. Sécurité dans l'espace et cybersécurité : Quels sont les enjeux et les défis courants associés à la cybersécurité et à la sécurité dans l'espace? Quels types de solutions pourraient être proposés relativement à ces défis?

Candidate avec des Doctorats :

3. Amélioration de l'architecture canadienne de contre-prolifération : Quelles propositions de politiques ou modifications législatives pourraient être élaborées pour combler les lacunes qui demeurent en matière de contre-prolifération?
4. Quelle approche est la plus susceptible de mener à un monde sans armes nucléaires : la négociation immédiate d'une convention sur les armes nucléaires *OU* la réalisation d'un processus graduel visant à négocier et à mettre en œuvre des instruments juridiques et des accords politiques complémentaires tels que le Traité de non-prolifération, le Traité d'interdiction complète des essais nucléaires, le Traité sur l'interdiction de la production de matières fissiles, etc.?

Listes de lecture proposées pour chaque sujet sont disponibles sur demande. Pour recevoir un exemplaire, s'il vous plaît communiquer avec Elaine Hynes à la Fondation Simons par courriel à ehynes@thesimonsfoundation.ca ou au numéro de téléphone 778-782-7779.

L'objectif premier de ces bourses consiste à accroître la recherche aux cycles supérieurs sur les enjeux liés au désarmement, au contrôle des armements et à la non-prolifération.