Brian David A. Mussington, PhD CISSP

Center for Public Policy and Private Enterprise
School of Public Policy
University of Maryland
2211B Van Munching Hall
College Park, Maryland
20742
bmussing@umd.edu

12155 Puddle Place
Nokesville, VA
20181-3640
703-367-0310 (Home)
571-247-2140 (Cell)
wintermute1@icloud.com (Email)

Profile

Internationally recognized expertise in information systems security, infrastructure protection, cyberspace operations analysis, military cyberspace and national security. Special expertise in critical transportation, financial services, and defense cyber threat and vulnerability management.

Education

Post-Doctoral Research, Harvard University, International Institute for Strategic Studies (IISS)
Ph.D. Political Science, Carleton University
M.A. Political Science (International Relations), University of Toronto
B.A. Economics and Political Science (Honors), University of Toronto

Certification: Information Systems Security Professional (CISSP) ID Number: 452745

Professional Experience

September 2019 -**Visiting Professor,** Security and Defense Hub/Cyber Policy and Critical Infrastructure Cybersecurity, Le CNAM (Paris),

March 2019 - **Research Associate**, Security and Defense Hub, Le CNAM (Paris, France)

December 2018 - **Elected Board Member**, The International Information System Security Consortium, $(ISC)^2$

July 2018 –**Member -** Verified Voting Technical Advisory Board

June 2018 – **Member** – Association for Computing Machinery (US) Technology Policy Committee

September 2016 – Present, Professor of the Practice, and Director, Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland

August 2016 – Present, **Senior Fellow**, Center for International Governance Innovation (CIGI)

- Focus Areas: Critical Infrastructure Cybersecurity and Resilience; US Cyber Policy, Military Cyber Doctrine and Cyber Threat Indications and Warning.

March 2015 – September 2016 – **Assistant Director**, Information Technology and Systems Division, Institute for Defense Analyses (IDA)

- Oversight of a project portfolio including research for the ODNI, DHS, DOD
- Project leadership on research addressing cybersecurity, critical infrastructure protection, cyber policy and risk management

January 2014 – March 2015 – Senior Vice President, Cybersecurity, Juno Risk Solutions
Engagement Role: Consulting CISO - **Director – Cybersecurity Strategy Initiative – Bank of Canada**

- Led a team Implementing a NIST- based Cybersecurity Framework for the Bank of Canada;
- Interface directly with executive management, gained and retained support for the initiative;
- Lead execution of a cybersecurity controls baseline and gap analysis;
- Design team lead on developing a Bank of Canada cybersecurity strategy;
- Senior advisor to senior deputy governor (no. 2 official at Bank) on organizational transformation for enhanced IT security governance and audit.

Key Achievements:

- Established a standards-based cybersecurity program for the Bank of Canada
- Led development of the first Bank of Canada Cybersecurity Strategy – completed and adopted by the Bank of Canada Cybersecurity Steering Committee in September 2014;
- Completed a gap assessment of cybersecurity preparedness and made recommendations for risk mitigation – using a methodology based on the 2014 NIST Cybersecurity Framework;
- Successfully devised 30-month risk mitigation program that includes governance, policy and technology investment phases. Adopted by Bank as policy in July 2014.

January 2013 – Present: **Adjunct/Research Staff Membe**r, Institute for Defense Analyses (IDA), Information Technology and Systems Division (ITSD)

Role: Lead on project for the US Department of Homeland Security on cyber threat information exchange and cyber-incident early warning. Provide subject matter expertise on critical infrastructure cybersecurity; public private partnerships for cyber security and resilience; industrial control systems security.

Key Achievements:

- Led a study of cyber threat data and information flows in critical infrastructures
- Devised an innovative DHS cyber threat data flows maturity model for critical infrastructures
- Facilitated evaluation of novel visual tool methods for representing cybersecurity information flow in and among critical infrastructures

December 2011 – January 2013 – **Director, Surface Transportation Security Policy**, Transborder Security Policy Directorate, National Security Council, Executive Office of the President (EOP), The White House.

Role: Oversight of national policy and strategy to enhance the security of surface transportation critical infrastructures including: freight and passenger rail systems, mass transit systems, and oil

and natural gas pipelines; Leadership of interagency planning to mitigate cyber-physical vulnerabilities in surface transportation infrastructure control systems; Alignment of DHS science and technology priorities with emerging threats and vulnerability exposure in transportation sector operating environments.

Key Achievements:

- Special activities relating to information assurance practices and vulnerabilities in the oil and natural gas sector; NSS-lead in working group on cyber-physical system risk identification and integration activity;
- National Security Council Staff (NSC) Transportation Security Policy Lead – Industrial Control System Cyber Security Initiatives and Coordination (Oil and Gas Pipeline Sector).

February 2010 – December 2011 – **Appointed to the Senior Executive Service (SES) – Assignment, Senior Advisor for Cyber Policy, Office of the Secretary of Defense (OSD)**.

Role: Thought leadership in cyber security policy and strategy development. Led a DOD-wide effort to define and pilot test a cyber mission assurance methodology and priority setting framework; leadership of telecommunications sector supply chain security activity; OSD Policy lead on internet technical standards and internet governance.

Key Achievements:

- Led development of DOD Defense Strategy for Operating in Cyberspace, signed by former Secretary of Defense Robert Gates, July 2011.
- Led development and pilot testing of a cyber mission assurance methodology for DOD weapons system and support infrastructure, including supply chain risk analysis for critical hardware and software systems.
- Led review within the Office of the Secretary of Defense (Policy) on DOD Cloud Computing Strategy and Plans (2011).

September 2009 – February 2010, **Chief of Corporate Security, National Railroad Passenger Corporation (Amtrak)**

Role: Led definition and management of Amtrak critical infrastructure protection project portfolio; initiated and led Amtrak Corporate Security's program management office (PMO), with 6 full-time program managers and over 20 project management contract staff implementing a portfolio of projects valued at over $500 million – enhancing the protection of Amtrak passengers, critical business and control systems, and facilities.

Key Achievements:

- Devised and implemented a security capital planning system allocating $450 million in infrastructure protection funding appropriated under the American Recovery and Reinvestment Act of 2009.
- Devised planning system to allocate residual TSGP funded and Amtrak internal capital-supported security infrastructure improvement projects
- Designated Sector Subject Matter Expert (SME) – National Academy of Sciences (Transportation Research Board).

August 2007 – September 2009, **Deputy Director - Policy and Programs at Office of Security Strategy and Special Operations (OSSSO), National Railroad Passenger Corporation (Amtrak)**

Role: Led development of corporate security, infrastructure protection, business continuity strategies and managed the program office implementing vulnerability and risk assessments for infrastructure protection projects for Amtrak's national railroad network. Coordinated counter-terrorism plans and emergency preparedness protocols with the Amtrak Police Department and managed the TSA Transit Security Grant Program.

Key Achievements:

- Established and led a program office for the Office of Security Strategy and Special Operations.
- Developed and implemented a program budget for the Amtrak Police Counter Terrorism Canine Response
- Achieved significant and measurable risk reductions in critical infrastructure segments of the Amtrak intercity rail system – hardened bridges and tunnels utilizing robust and standardized risk reduction metrics.
- Streamlined Amtrak grant submission and project design for activities supported under the TSA Transit Security Grant Program;
- Reviewed and revised Amtrak Police Department Asset Forfeiture spending for critical infrastructure protection;
- Selected as the senior official representing Amtrak on the Security Risk Management Committee of the American Public Transportation Association (APTA)

July 2006 – August 2007, **Senior Principal Officer – Security Evaluations and Intelligence**, National Railroad Passenger Corporation (Amtrak) – Office of Inspector General

Role: Counter-Terrorism Program Oversight, Security Reviews and Security Standards Identification and Development, senior official in charge of security evaluations and special advisor to the Inspector General.

August 2004 – 2006, **Adjunct Faculty**, Security Studies Program (SSP), Georgetown University, Edmund A. Walsh School of Foreign Service, Georgetown University, teaching seminars on Information Operations and Information Warfare, International Relations

October 1995 – July 2006 - **Political Scientist,** RAND Corporation

Research Specialization: Information Assurance and Information Security, Homeland Security and Counter-Terrorism, Critical Infrastructure Protection, Terrorist Finance

Role: Study Principal Investigator and Research Scientist

Key Achievements:

- 2005: Adoption of 44 substantive recommendations, and implementation in a new Corporate Security (infrastructure protection focus) department at the National Railroad Passenger Corporation (Amtrak).
- 2004: Principal investigator on the first comprehensive assessment of the vulnerability of the US intercity passenger rail system to mass casualty terrorism.

- 2000: Principal Investigator: Y2K Lessons-Learned Study for White House Office of Science and Technology Policy (OSTP)
- 1997-1999: Team Member – Day After … simulations on cybersecurity and financial crime. Implemented for Defense, the Treasury and State Departments.

Awards and Honors

Certified Information Systems Security Professional (CISSP) Certification, ID No. 452745 (June 2013-2016)

Department of Defense – Office of the Secretary of Defense Group Achievement Award, Contributions in Support of DoD Strategy for Operating in Cyberspace (DSOC), July 2011.

Post-Doctoral Fellow, Belfer Center for Science and International Affairs (BCSIA), John F. Kennedy School of Government, Harvard University.

Harvard MacArthur Scholar **and Research Fellow, Center for International Affairs (CFIA), Harvard University.**
Publication: Arms Unbound: The Globalization of Defense Production (Cambridge, MA: CSIA Studies in International Security No.4, Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University/Brasseys (US) 1994).

Research Associate, International Institute for Strategic Studies, (IISS) - (UK)
Publication: Understanding Contemporary International Arms Transfers, *Adelphi Paper 291,* (London: IISS/Brasseys, September 1994).

Visiting Professor, Monterey Institute of International Studies (MIIS); Co-Director, International Organizations and Non-Proliferation Project (IONP), Center for Non-Proliferation Studies.
Publication: *US Foreign Economic Policy and High Technology Industries: The Case of Imaging and Satellite Technologies* (Monterey, CA: Center for International Trade Strategy, MIIS, September 1995).

Professional and Other Activities

Member: The International Institute for Strategic Studies (IISS)
American Political Science Association
The Internet Society
Association for Computing Machinery (ACM)
AFCEA
Verified Voting Foundation
Election Verification Network (EVN)
ISC2

PUBLICATIONS AND REPORTS

BOOKS AND MONOGRAPHS

"Strategic Stability, Cyber Operations and International Security" in Aaron Shull (Ed.)
Governing Cyberspace During a Crisis in Trust (Ottawa: Center for International Governance Innovation, 2019), (https://www.cigionline.org/publications/governing-cyberspace-during-crisis-trust)
Accessed 21 June 2019.

The Missing Compliance Framework in the 2015 US-China Cybersecurity Agreement, (IDA Non Standard NS D-5648), November 18, 2015

Strategic Analysis of Cyber Threat Information Flows (with S. Katharine Burton, Michelle Alberts, R. James Caverly, Jemakai Blyden, Louise Davidson, Becaja Caldwell, Rachel Greenspan, (Alexandria, VA: IDA), 2014

A Review of Approaches to Sharing or Relinquishing Agency-assigned Spectrum, with Karen D. Gordon Jonathan R. Agre, Daniel K. Correa, Bill Brykczynski, J. Katharine Burton, Leo H. Jones, Jr., Michael C. Mineiro, (IDA Paper P-5102), (Alexandria, VA: IDA, January 2014)

"A Cyber Threat Information Sharing (CTIS) Framework", Working Papers, (IDA), September 2014

Exploring Money Laundering Vulnerabilities through Emerging Cyberspace Technologies: A Caribbean – Based Exercise (with Peter A. Wilson and Roger C. Molander), (Santa Monica, CA: RAND), MR-1005-OSTP/FinCEN, 1998.

Explorando Las Vulnerabilidades Del Lavado Del Dinero Por Medio De Las Tecnologias Emergentes Del Ciberespacio: Une Ejercio De Base Caribeno. (With Peter A. Wilson and Roger C. Molander), (Santa Monica, CA: RAND), MR-1005/1-OSTP/FinCEN, 1998.

Strategic Information Warfare Rising (with Roger C. Molander, Peter A. Wilson, and Richard F. Mesic), (Santa Monica, CA: RAND), MR-964-OSD, 1998.

Cyberpayments and Money Laundering: Problems and Promise (with Roger C. Molander and Peter A. Wilson), (Santa Monica, CA: RAND), MR-965-CTI, 1998.

US Foreign Economic Policy and High Technology Industries: The Case of Imaging and Satellite Technologies (Monterey, CA: Center for International Trade Strategy, Monterey Institute of International Studies, September 1995).

Arms Unbound: The Globalization of Defense Production (Cambridge, MA: CSIA Studies in International Security No.4, Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University/Brasseys (US) 1994).

Understanding Contemporary International Arms Transfers, *Adelphi Paper 291,* (London: IISS/Brasseys, September 1994).

Public Health Preparedness in California: Lessons Learned from Seven Health Jurisdictions with Nicole Lurie, R. Burciaga Valdez, Jeffrey Wasserman, Michael Stoto, Sarah Myers, Roger Molander, Steven Asch, and Vanessa Solomon (Santa Monica, CA: RAND), August 2004

Issues in Amtrak Security [DRR 3339], with Anny Wong (Santa Monica, CA: RAND), June 2004

Two Concepts for Improving Capabilities in Information Security/Information Assurance (for the White House Office of Science and Technology Policy), (Santa Monica, CA: RAND), August 2002

Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development (Santa Monica, CA: RAND) Science and Technology Policy Institute, MR-1259-OSTP, 2002

Research and Development Challenges in Critical Infrastructure Protection (for the White House Office of Science and Technology Policy), (Santa Monica, CA: RAND), PM-1034-STPI, February 2000.

The 1999 US-UK "Day After" Critical Infrastructure Protection (CIP) Exercise, with Roger Molander et al., (Santa Monica, CA: RAND), PM-1019-OASD (C3I), December 1999.

On the Eve of Y2K: An Interim Integrated Look at the Y2K Problem, with Roger Molander et al., (Santa Monica, CA: RAND), PM-1022-NIC, December 1999

The Day After…Y2K After-Action Report, with Roger Molander, Peter Wilson, Jennifer Brower, Richard Mesic, Robert Anderson, and Orlie Yaniv (for the National Intelligence Council) (Santa Monica, CA: RAND) PM-964, July 1999.

Identifying Potential Institutional Problems in Critical Infrastructure Protection Policy, (Santa Monica, CA: RAND), PM-982-STP, September 1999.

PEER REVIEWED ARTICLES

"Countering 'Made in China 2025': Strategy for Western Powers in a Cybered World," Military Cyber Affairs, Vol. 3: Issue 2, Article 2 (March 2019). https://scholarcommons.usf.edu/mca/vol3/iss2/2 Accessed 9 March 2019 (Peer Reviewed)

"Transnational Challenges and the International Security Environment," (with William Rosenau and Kemper Gay), Law Enforcement and Low Intensity Conflict, 3,1, (1998).

"Defense Conversion and Industrial Competitiveness in the United States: A New Test for Industrial Policy," Business and the Contemporary World," 2,1995, pp. 146-156. "The International Control of the Arms Trade," Revue Beige De Droit International, 1993/1, pp. 53-57.

"Foreign Policy Latitude and Consensus Formation in the Western Security Community After the Cold War," in Frank Miceli, ed., The Security Reader, Columbia University (New York: Institute for War and Peace, Columbia University, Spring 1992).

"International Studies: Authentic Paradigms and the Necessity of Choice," International Studies Notes, 14,2 (Spring 1989), pp. 45-49.

CHAPTERS IN EDITED VOLUMES

"Securing the Critical National Infrastructure (Including the Essential Role of the Private Sector)", in Paul Cornish (Ed.) *The Oxford Handbook of Cyber Security* (Oxford and London: Oxford University Press, 2019), Forthcoming.

"Strategic Stability, Cyber Operations, and International Security" in Aaron Shull (Ed.) *Governing Crisis During a Criss of Distrust*, (Ottawa: Center for International Governance Innovation (CIGI), 2019), pp. 55-60.

*"*Cyber Terrorism and Homeland Security," in David Charters, (ed.) *Asymmetric Strategies, Homeland Security, and Public/Private Sector Responses*. (Fredericton, NB: University of New Brunswick, Canada 2005).

*"*The Day After Methodology and Defense Analysis," in Greg Treverton (ed.) *Defense Analysis Methods for the New Century*, (Santa Monica: RAND, 2002).

*"*Asia Defense Policy and Procurement Trends," and "Information Warfare," in JR Wilson (ed.,) *Defense and Security Review 1998* (London: Atalink Publishing, 1998).

*"*Asia Defense Policy and Procurement Trends," in JR Wilson (ed.,) *Defense and Security Review 1997* (London: Atalink Publishing, 1997), pp. 24-29.

*"*Contending Models for Preventing Excessive and Destabilizing Arms Buildups," in Andrew Latham

(ed.,) *Multilateral Approaches to Nonproliferation* (Toronto: York University Centre for International And Strategic Studies, 1996), pp. 19-33.

"The Imperatives for Cooperation." (with Nolan, Janne E., John D. Steinbruner, Kenneth Flamm, Steven E. Miller, David Mussington, William J. Perry, and Ashton B. Carter.) In *Global Engagement: Cooperation and Security in the 21st Century ,* ed . Janne E. Nolan . Washington, DC: The Brookings Institution, 1994.

PERIODICAL ARTICLES

"Financial Institutions Must Not Ignore Risks of Cryptocurrencies." **Toronto Globe and Mail** 26 February 2018 https://www.theglobeandmail.com/report-on-business/rob-commentary/financial-institutions-must-not-ignore-risks-of-cryptocurrencies/article38122059/ [Op Ed]

Accessed 9 March 2019

*"*Protecting Critical Infrastructure", *RAND Research Review*, (July 2002).

*"*The Emergence of Electronic Money," *Compuweb*, (October 1996), http://www.pollux.com.

*"*Throwing the Switch in Cyberspace," *Jane's Intelligence Review*, (July 1996), pp. 331-334.

CONFERENCE PAPERS, PRESENTATIONS AND BRIEFINGS

"The Requirement for Better Data and Analytical Frameworks for Cyber Operations Assessment and Risk Management," AAAS Annual Meetings, Washington DC 13-15 February 2019

"Fake News vs. Censorship: How can Democacies Regulate the Information Battle?" for The Digital Society Conference 2018: Empowering Ecosystems, Digital Society Institute (DSI), Berlin Germany December 10-11 2018.

"Election Cybsersecurity, Cyber conflict, and U.S. National Security", Penn State Symposium on Election Security, hosted by the College of Engineering, the Penn State Law and the School of International Affairs, and the Institute for Cyber Science. 3 December 2018. [Invited Keynote] (https://www.eecs.psu.edu/news/2018/election-cybersecurity-symposium.aspx) Accessed 9 March 2019

"Election Security and Cyber Conflict: Understanding the New Normal", presented at the National Committee on American Foreign Policy (NCAFP), New York City, 16 November 2018. [Invited Speaker]

"Cybersecurity and US Elections: Where Do we Stand? (A Framework for Answers)" River Road Unitarian Congregation 21 October 2018 [Invited Speaker]

"Election Cybersecurity: Lessons from 2016", presented at the CSG/ERG (Council of State Governments/Eastern Region) Annual Meeting, August 7-9, 2018.

"Cybersecurity and the 2016 US Presidential Elections", delivered at Invited Cross Divisional Seminar Briefing, Institute for Defense Analyses, July 26 2018 [Invited Presentation]

"Framing the Global Cyber Landscape and Mapping Response Strategies", CyberCanada Senior Leadership Summit, 28 February – 1 March 2018. [Panelist and Invited Speaker]

"Fostering Defense Cyber Innovation – Aligning Offense and Defense," Prepared for The Digital Society Conference 2017: Reliability Reloaded organized by the Digital Society Institute (DSI), November 20-21, 2017 Berlin Germany

"Eligible Receiver at 20 – Enduring Mearning of a Foundational Exercise," 12 November 2017 (LinkedIn url) / (https://www.linkedin.con/pulse/eligible-receiver-20-enduring-meaining-foundational-b-david/ Accessed 9 March 2019

"Mutually Assured Disruption", hosted at National Committee on American Foreign Policy (NCAFP), 12 October 2017. [Panelist and Invited Speaker]

"Cyber Risk Management at the Bank of Canada: Implications and Lessons Learned," Institute for Defense Analyses (IDA), Cross Divisional Cyber Seminar, 21 December 2015

"Cybered Alliances, Spheres, and Independents; (CASI)" *Third Biennial Workshop: Cybered Futures and Conflict/Governance Implications*, US Naval War College, 22 September 2015

"Cyber-Terrorism and Homeland Security," *Terrorism, Asymmetric Warfare and Homeland Security: Understanding the Issues One Year After 9/11.* The Wu Conference Center, University of New Brunswick, Fredericton, NB E3B 5A3. October 4-5, 2002.

"Critical Infrastructure Protection: Securing the Banking and Financial Services Infrastructure", Naval Postgraduate School, 16/18 July 2002.

"Potential Abuse in the Digital Economy: Research and Analytical Insights," (with Roger Molander and Peter A. Wilson), Invitational Briefing hosted by Racketeering and Audit Unit, Federal Bureau of Investigation Laboratory, 18 February 1999.

"The Financial Crimes Enforcement Network (FinCEN)-RAND Simulation Exercise", with Dr. Roger Molander. *Sixth Annual Fraud and Enforcement Training Conference*, Arlington, VA. October 8, 1997. Sponsored by the Federal Deposit Insurance Corporation.

"The Shifting International Economic and Political Context of Remote Sensing" May 5-10, 1997 Bremen, Germany (4th International Space Congress), Presentation and Discussant Remarks.

"The Proliferation Challenges of Cyberspace," presented *at Cyberspace and Outerspace: NACD in the 21st Century*, Ottawa, Government Conference Center, March 3-6, 1997. Hosted by the Department of Foreign Affairs and International Trade, Government of Canada.