THE CYBER-NUCLEAR NEXUS

NIAMH HEALY, UNIVERSITY COLLEGE LONDON
“In operational testing, [the US Department of Defense] routinely found mission-critical cyber vulnerabilities in systems that were under development, yet program officials GAO met with believed their systems were secure and discounted some test results as unrealistic”

– Government Accountability Office [GAO] Report to the Committee on Armed Services, US Senate, October 2018
AGENDA

• Defining the problem
  – Cyber? Nuclear?
• Understanding the problem
  – Case study: NC3
• How can we address the problem
  – Unilateral, bi/multilateral measures
Cyber?

- Cyberspace: “all computer systems and networks in existence, including air-gapped systems” (Kello)
- Cyberattack: “the use of code to interfere with the functionality of a computer system for a political or strategic purpose” (Kello, emphasis added)
- Cyberspace both an attack vector and a sphere of operations (Dunn-Cavelty)
Nuclear?

• Nuclear order
  – “Given the existence of nuclear technology, the international nuclear order entails evolving patterns of thought and activity that serve primary goals of world survival, war avoidance and economic development” (Walker, emphasis added)

• Two linked systems to achieve this
  – System of deterrence
  – System of abstinence
So if we have set up these political systems around nuclear weapons to “serve primary goals of world survival, war avoidance and economic development” (Walker, emphasis added),

how will developments in cyberspace disrupt them?
• Central idea of nuclear deterrence: don’t attack us or we’ll attack you
• Cyber-attack affecting nuclear command, control and communications (NC3)?
• Examples:
  – Tampering with infrared sensors intended to detect ballistic missiles (within the supply chain)
  – Jamming or spoofing satellite communications
• These attacks could impede communication between:
  – Early-warning systems and National Command Authority (NCA)
  – NCA and nuclear weapons operators
  – NCA and diplomatic counterparts
HOW CAN ADDRESS THE PROBLEM

UNILATERAL
• Separate out conventional and nuclear systems
• Building in more decision-making time to nuclear postures
• Prioritizing cybersecurity in procurement / supply-chain and culture

BILATERAL OR MULTILATERAL
• Nuclear weapons states pledge not to attack one another’s NC3 systems
• Cyber incident hotlines
CONCLUSION

• Activity in cyberspace is changing nuclear order, increasing risks around nuclear weapons
• We still don’t fully understand in what ways cyber is impacting nuclear order
  – Non-proliferation?
• There are things nuclear weapons states can do to reduce risk in this area
BIBLIOGRAPHY

• Andrew Futter, Hacking the Bomb: Cyber Threats and Nuclear Weapons (Georgetown University Press, 2018)
• David Livingstone, and Patricia Lewis, Space, the Final Frontier for Cybersecurity? (Chatham House, September 2016) [https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf]
• John Gower, United Kingdom: Nuclear Weapon Command, Control, and Communications (Nautilus Institute, 12 September 2019) [https://nautilus.org/napsnet/napsnet-special-reports/united-kingdom-nuclear-weapon-command-control-and-communications/]
• Lucas Kello, The Virtual Weapon and International Order (Yale University Press, 2017)
• Page O. Stoutland, and Samantha Pitts-Kiefer, Nuclear Weapons in the New Cyber Age (Nuclear Threat Initiative, 26 September 2018) [https://www.nti.org/analysis/reports/nuclear-weapons-cyber-age/]
— — —, ‘Nuclear Order and Disorder’, International Affairs (Royal Institute of International Affairs 1944-), 76.4 (2000), 703–24