Chapter 1: Emerging Threats in the AI Era

Blueprint for Action: Number One

Combating Malign Information Operations Enabled by AI.

The use of AI to produce, manipulate, and promote malign information marks a disruptive evolution in the use of information as a tool of statecraft, a weapon of war, and a threat to democracy.[1] The following recommendations represent a strategic, organizational, and operational framework that the U.S. government should adopt to adequately defend and counter malign information operations in the AI era, including by employing AI-enabled technologies.

Recommendation

Recommendation: A National Strategy for the Global Information Domain

Expanding upon the principles of information statecraft outlined in the 2017 National Security Strategy,[2] the President should issue a new national strategy for the global information domain that more fulsomely addresses how AI and associated technologies are defining new fronts in this area. The strategy should:

- Acknowledge that the network-connected world is dissolving barriers between societies.
- Prioritize the global information domain as an arena for competition.
- Detail how adversarial state and non-state actors are attempting to define and control the global information domain in order to shape global opinion and achieve strategic advantage.
- Account for the critical role of AI-enabled malign information in achieving these goals.
- Designate malign information operations as a national security threat with its own set of priority actions to defend, counter, and compete against them.
- As necessary, update critical infrastructure designations and require relevant departments and agencies to update sector-specific plans to reflect emerging technologies.
- Establish organizational structures for U.S. national security agencies to defend, counter, and compete against the threat.

Action for the President:

- Issue a supplemental National Strategy for the Global Information Domain.

Action for Congress:

- Congress should direct the Executive Branch to transmit a National Strategy for the Global Information Domain that categorizes the global information domain as an arena of competition vital to the national security of the United States.

Organizational Framework

The proliferation of malign information has exposed an Achilles heel in the U.S. national security apparatus. Previous major reorganizations could not foresee contemporary digital technology and society's profound dependence upon it. They could not anticipate the use of ICT platforms and tools, bots, and AI-enabled technologies to spread false information. They do not account for the role that the commercial sector and civil society play in defending against malign information, and enabling its spread. Individual agencies such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) have stretched their mandates to confront the threat. They rely on narrow sets of outdated tools, and are hampered by cultures shaped by the Cold War and counter-terrorism paradigms.

Recommendation: Create a Joint Interagency Task Force (JIATF) and Operations Center.

Recommendation

Action for the President:

- **Direct creation of a JIATF and operations center to lead and integrate government efforts to counter foreign-sourced malign information in real time.**
    - The Presidential action should direct the Secretaries of State, Defense, Justice, and Homeland Security, the Attorney General and the Director of National Intelligence, to create a JIATF and stand-up an operations center to counter foreign-sourced malign information.
    - The JIATF should integrate efforts of key offices, bureaus, and divisions within each of these agencies, as well as the broader intelligence community (IC) and law enforcement establishment.
    - The JIATF should have the responsibility to survey the landscape of relevant public and private actors, coordinate among them, and act in real time to counter foreign information campaigns.
    - The JIATF should draw on existing authorities to create an operations center with modern, AI-enabled digital tools and expert staff to expose, attribute, and respond effectively.
    - The Presidential action should also direct these officials, as part of the JIATF, to create a mechanism to share and exchange critical information with key companies in the private sector that run internet and social media platforms where malign information proliferates.

Action for the Secretaries of State, Defense, Justice, Homeland Security, and the Director of National Intelligence:

- **Establish the JIATF and Operations Center.**
    - These agency heads should direct immediate development of a plan to create the JIATF and operations center with a focus on identifying those offices, bureaus, and divisions within their agencies and the broader IC and law enforcement establishment that are essential to the mission of countering foreign-sourced malign information.
        - As part of this effort, the JIATF should leverage the authority provided by Congress in the FY2020 NDAA to stand-up a Foreign Malign Influence Response Center within ODNI.[3]
        - Components that will be critical to the JIATF include, among others, the Central Intelligence Agency's Open Source Enterprise and the National Counterintelligence and Security Center.[4] Leadership will need to ensure involvement of relevant components from the FBI, the National Security Agency, across the Department of Defense, and the Global Engagement Center (GEC) at the Department of State.
- The JIATF would lead and integrate existing and new national strategic efforts against foreign malign information operations by providing analysis, sharing information with government and commercial partners, and driving whole-of-government *action*, subject to Presidential direction, to advance U.S. information objectives.
- The Commission proposes that the operations center component of the JIATF be modeled on the National Counterterrorism Center (NCTC), as a proven model for providing real-time situational awareness of and response to evolving national security threats.
- To exchange information and coordinate with internet and social media platforms on malign information threats, the Commission proposes creation of an associated industry consortium that includes an information sharing and analysis center (ISAC). The consortium, supplemented by the ISAC, would allow the JIATF to exchange information *with industry*, monitor malign information across ICT platforms, and improve U.S. government response to malign information threats. In developing the ICT consortium and ISAC, JIATF should look to the Global Internet Forum to Counter Terrorism as a model.[5]

Action for the Director of National Intelligence:

- **Appoint a Malign Information Threat Executive (MITE) to lead the JIATF.**
    - In July 2019, ODNI created the Election Threat Executive position responsible for coordinating across the IC on issues related to election security.[6] The threat of foreign malign information operations demands that this position be elevated, renamed, and expanded beyond the subject of elections.
    - The MITE role should also serve as a liaison function between the White House/ National Security Council and the JIATF to ensure alignment and responsiveness to the national security strategy.

Action for Congress:

- **Appropriate $30 million per year to support the operations of the JIATF.**

Operational Framework

Efforts by the U.S. Government and private sector to counter terrorist propaganda offer a potential roadmap for how the United States can go on the offensive to counter and compete against malign information. The creation of the Global Coalition to Defeat the Islamic State of Iraq and Syria (ISIS) has shown how a burden-sharing model can be deployed to successfully counter and defeat a shared threat.[7] The United States and its allies will only succeed if they can develop and deploy personnel as well as an advanced set of tools to assist in their effort to counter and compete against malign information operations. Efforts need to be made to encourage innovation as well as harness commercially available technologies to go on the offensive.

Recommendation

Recommendation: The Department of State should lead a global effort to counter disinformation.

Action for the President:

- **Designate the Under Secretary of Public Diplomacy and Public Affairs at the Department of State to lead the international fight against malign information operations.**

Action for the Department of State:

- **Build an International Task Force to Counter and Compete Against Disinformation.** Modeled after the Global Coalition to Defeat ISIS, the Department of State should build a similar task force to counter malign information. The International Task Force to Counter and Compete Against Disinformation should be led by the Department of State's Under Secretary for Public Diplomacy and Public Affairs, with the GEC coordinating its daily activities.[8] The task force will be in charge of directing, leading, synchronizing, integrating, and coordinating efforts by allies to recognize, understand, expose, and counter foreign state and non-state propaganda and malign information efforts. The GEC should leverage the work of the Technology Engagement Team (TET) to share and test technologies to detect and disrupt the creation, manipulation, and dissemination of malign information from state and non-state actors. *See the Chapter 15 Blueprint for Action for more detail on creating a task force as part of the Emerging Technology Coalition proposed by the Commission.*

Recommendation

Recommendation: The Defense Advanced Research Projects Agency (DARPA) should coordinate multiple research programs to detect, attribute, and disrupt AI-enabled malign information campaigns and to authenticate the provenance of digital media.

The government should sponsor research to develop technologies to detect, attribute, and disrupt malign influence operations, including influence campaigns, psychological operations on social media platforms, and manipulated and synthetic media. In parallel,

the government should develop alternative technologies to authenticate the provenance of digital media and head off the risk that other approaches will not be successful. These efforts should be led by DARPA.

Action for Congress:

- **Appropriate $60 million to $80 million in additional funding for DARPA to sponsor multiple research projects to develop technologies to detect, attribute, and disrupt malign influence operations that rely on AI-generated content, and to develop alternative technologies to authenticate the provenance of digital media.**[9] DARPA has existing authority to fund such research with the scope outlined in this recommendation, but will require dedicated appropriations to carry out the effort and a security review of the best innovation vehicles to sponsor the research.

Action for DARPA:

- **Sponsor further research as described above using innovation vehicles, such as challenge competitions, or any other deemed necessary by DARPA to develop and transition these technologies to accountable agencies and departments for maximum employment.**

Recommendation

Recommendation: Create a task force to study the use of AI and complementary technologies, including the development and deployment of standards and technologies, for certifying content authenticity and provenance.

In response to the challenges of misinformation, efforts are underway to develop standards and pipelines aimed at certifying the authenticity and provenance of audiovisual content.[10] These efforts make use of technologies, including encryption and fragile watermarking, to secure and track the expected transformations of content via production and transmission pipelines. These efforts offer the opportunity to mitigate malign information campaigns that seek to corrupt or spoof highly trusted sources of information across our digital ecosystem. This technology area is ripe for public-private partnership, as several private organizations are already forming to fight disinformation.[11]

Actions for the Office of Science and Technology Policy (OSTP):

- **Establish a task force to study the use of AI and complementary technologies for certifying content authenticity and provenance.**
    - OSTP should establish an interagency task force to assess the use of AI and complementary technologies to certify content authenticity and provenance, to include an evaluation of technical standards and production and transmission pipelines.
    - The task force should make recommendations on methods to improve content certification, which may include public-private initiatives, legislation, and changes to federal policy. In addition, the task force should assess options for federal regulation of content certification by non-governmental organizations.

Recommendation

Recommendation: Executive Branch departments and agencies should utilize Other Transaction Authorities (OTAs), creative investing, and the Small Business Innovation Research (SBIR) program to deploy capital to companies that offer technical solutions that will assist the United States Government in identifying, countering, and defending against malign information operations.

The U.S. Government has an array of mechanisms that are not currently leveraged to deploy capital to companies that create strategic technology to unleash AI, machine learning (ML), and associated technologies in this counter-information operations fight.[12]

Action for all U.S. departments and agencies:

- **Explore the use of the SBIR program and OTAs to acquire technology solutions that will assist the United States Government in identifying, countering, and defending against malign information operations.**

The United States must prepare for both the present and future threat of increasingly automated and AI-enabled cyber conflict. The expanding threats of mutating malware and AI-powered tools are combining with traditional cyber threats to automate, optimize, and ultimately transform the precision, speed, stealth, scale, and effectiveness of cyber-attack and espionage campaigns.[13] To defend the U.S. from current and future cyber threats, we must move to develop AI-enabled cyber defenses and to mitigate proliferating cyber vulnerabilities.

Chapter 1: Emerging Threats in the AI Era

Blueprint for Action: Number Two
Preparing for AI-Enabled Cyber Conflict.

Section 1: Developing AI-enabled defenses against cyber attacks.

Recommendation

Recommendation: Develop and deploy machine-speed threat detection and mitigation.

Detecting and reacting to unknown threats on a network is difficult, but not impossible, for self-learning AI systems that have been trained to differentiate between normal and anomalous network behavior.[14] To address deficiencies highlighted by the SolarWinds attack, autonomous defenses are needed to defend the U.S. Government's systems.

Actions for the Department of Homeland Security and Department of Defense:

- **Expand machine speed threat information sharing, behavior-based anomaly detection, and cyber threat mitigation to all government networks containing sensitive information and critical functions.**
    - DHS must improve the National Cybersecurity Protection System (NCPS), while DoD must also accelerate its efforts to harness AI-enabled cyber defenses and sensors. At a minimum, the objective of these new defenses should be to flag or potentially block never-before-seen connections and communications missed by currently deployed intrusion detection and prevention technologies such as EINSTEIN.[15] To fully take advantage of new capabilities, these defenses should also aim to accelerate recovery from cyber attack by automatically generating courses of action for federal agencies to assure secure continuity of operations. These defenses should assist recognition of insider threats as well as externally launched attacks, and use machine speed information sharing to prepare other public and private networks to defend themselves against detected threats.
    - DoD and DHS must also assess and mitigate security risks posed by introducing and enhancing threat detection systems. These systems will require precautions against their elevated system access being used to deliver malware or abused by other cyber threats. AI-enabled system components designed to mitigate new and unknown threats likewise will need defenses against adversarial techniques.
    - To minimize cost overruns in altering a multibillion-dollar project, DHS should reprogram $10 million to investigate the best means to accelerate and set up AI-enabled threat detection systems. This study would be tasked to look for synergies with existing intrusion detection software and infrastructure, seek to address any remaining key deficiencies found by GAO in the National Cybersecurity Protection System, and to develop a final budget proposal for Congress.[16] This study likewise should aim to address how previous intrusion detection systems failed to detect the SolarWinds cyber attack.

Recommendation

Recommendation: Execute large, instrumented, and realistic tests to gather data and train AI-enabled cyber defenses.

AI-enabled cyber defenses require training to recognize potential threats, and sensors to detect them. By experimenting with larger networks in realistic conditions, the United States can train more robust AI-enabled cyber defense capabilities.

Action for Congress:

- **Fund the Defense Advanced Research Projects Agency (DARPA) to sponsor additional secure, instrumented, and realistic research on AI-enabled cyber defenses.**
    - DARPA funding should be increased by $20 million, to be divided between a security review, and other programmatic costs for the additional research. DARPA should be left free to determine the structure of further research, with an innovation vehicle such as a challenge competition or any other that DARPA deems necessary.
- **Expand the National Institute of Standards and Technology AI testbed program.**

- For FY2021, NIST requested a $25 million increase, for measurement tools and testbeds to accelerate the development and adoption of interoperable, secure, and reliable AI technologies.[17] Since then, NIST has been authorized for $64 million in additional AI R&D responsibilities including AI testbeds. To ensure NIST can meet its new responsibilities in addition to its prior ones, Congress should meet NISTs authorized funding increase for AI R&D.

Actions for DARPA:

- **Structure and standardize an innovation vehicle, such as a challenge competition, or any other DARPA deems necessary, to increase insight about options for new AI-enabled cyber defenses.**
  - DARPA should aim to encourage the prototyping of new means of AI-enabled cyber defense and test the efficacy of these defenses against intelligent opponents and AI-enabled cyber threats. DARPA should structure new research to broaden insight on the importance of real-life factors such as cyber-attack externalities, differences in risk tolerance between threat actors, and differences in network infrastructure between defenders.[18]
- **Bring broader fields of expertise to bear for cyber defense research.**
  - Cyber expertise is not the only expertise relevant to cybersecurity and the efficacy of cyber operations.[19] The new research should involve experts from other fields such as economics, game theory, and behavioral psychology to improve scoring metrics, improve the human components of cyber strategy, and propagate insight further within government. With these improved metrics and insights, future investments can be more directly aligned with mission assurance.
- **Conduct a security review to determine the rules and bounds of new cyber research initiatives.**
  - DARPA must conduct a thorough security review about the second-order effects of sponsoring research with public-facing results and without strong information security measures, to mitigate against potential adversaries acquiring information that can be weaponized against us. International competition in this area is getting so intense that the organization must consider using a vetted closed-challenge competition or initiative as opposed to an open-challenge competition format.

Actions for NIST:

- **Expand the NIST AI testbed program to generate data for AI-enabled cyber defenses in differing IT infrastructure environments.**
  - Larger-scale testing is necessary to generate the data required for AI-enabled cyber defenses. By scaling testbeds within NIST, there will be the opportunity to generate this data, and to evaluate the performance of varying network architectures at strengthening network security.
  - Training data often reflects a broad sampling of common scenarios and does not itself necessarily convey the costs of different types of compromises without further labeling.[20] *NIST should create optimized data sets for training cyber defenses to minimize expected costs of network disruption, compromise, and damage* rather than merely trying to identify cyber threats and vulnerabilities with high accuracy. To develop these data sets, NIST will need to hire or contract multidisciplinary talent to develop better metrics.

Recommendation

Recommendation: Ensure the robustness of AI-cyber defenses.

To make AI-based cyber defenses stronger, their supporting supply chains and data must be defended, while the algorithms themselves must be protected from malware, trained against adversarial techniques, and red teamed to the point of failure. *This approach can be found in the Chapter 7 Blueprint for Action.*

Section 2: Ensuring resilience against AI-enabled cyber attacks.

Many of the defenses required to protect against AI-enabled cyber threats are also required to defend against less advanced cyber threats. To provide this protection, the Commission endorses specific Cyberspace Solarium Commission recommendations, which are instrumental in enhancing U.S. defenses against AI-enabled cyber threats.[21]

Recommendation

Recommendation: Improve incentives for information and cyber security.

AI cannot defend inherently indefensible digital infrastructure against escalating offensive AI-enabled cyber capabilities. Even if vulnerabilities are known and easily patchable, that is no guarantee that they will be closed without a further impetus to action. Similarly, while new instrumented digital infrastructure is required to accelerate AI-enabled cyber defenses, those that build it must be careful to ensure new vulnerabilities don't outweigh the benefits of these defenses. In both cases, incentives must be realigned in the public and private sector to assure gaps are closed and new infrastructure is secure.

Action for Congress:

- **Establish liability for final goods assemblers for damage stemming from incidents that exploit known and unpatched vulnerabilities, incentivize reporting, and amend the Sarbanes-Oxley Act to include cybersecurity reporting requirements.[22]**
    - The Cyberspace Solarium Commission made recommendations to incentivize timely vulnerability patching. In addition to these recommendations, companies should be incentivized to improve their cybersecurity, and participate in new vulnerability disclosure programs via selectively reducing legal liability and product recalls for companies that can mitigate and patch controlled vulnerabilities within a limited, but rule-defined, time period. The overall structure of liability reform should aim to minimize perverse incentives to avoid liability by concealing failure. Grid, critical infrastructure, and medical device companies should be the primary targets for improvement.
    - To harmonize and clarify cybersecurity oversight and reporting requirements for publicly traded companies, Congress should amend the Sarbanes-Oxley Act to explicitly account for cybersecurity.[23]

Action for the Executive Branch

- **Incentivize information technology security through Federal Acquisition Regulations and Federal Information Security Management Act authorities.[24]**
    - Zero-trust networking and robust code should become key priorities for government contracts related to information technology, and especially for contracts related to AI. Contractors should not be paid more for additional lines of code when adding them generates new vulnerabilities without additional functionality. Code should be subjected to AI-enabled vulnerability review.
- **Task CISA to develop an IT infrastructure "Cash for Clunkers" incentive plan, to submit to Congress for FY2022.**
    - This program would support the replacement of vulnerable outdated equipment with modern alternatives through targeted federal subsidies. CISA should coordinate the effort by setting the program's strategy, prioritizing devices and critical digital infrastructure for replacement, and determining subsidy levels for the systems to be replaced. CISA must develop the plan so as to minimize perverse incentive to acquire vulnerable infrastructure before the plan is funded, and once the plan is developed, Congress must implement it as quickly as possible to reduce perverse incentives for companies to hold out on replacing vulnerable devices and infrastructure in the meantime.

Section 3: Disrupting adversary AI-enabled cyber-attacks and capabilities.

Recommendation: Develop additional, impactful non-kinetic options to respond to adversarial cyber and information operations.

Recommendation

Modern information operations have enormous overlap with cyber operations. As AI-enabled cyber capabilities spread in the presence of wide-open societal vulnerabilities, the United States needs to have additional tools to counter proliferating threat actors, and to establish deterrence in the cyber and information domains.

Action for Congress:

- **Expedite the establishment of the Bureau of Cyberspace Security and Emerging Technologies (CSET) within the U.S. Department of State.**
    - The CSET Bureau will be essential for strengthening norms in cyberspace, engaging other countries on information technology standards, assisting allied cyber defense, and improving international cyber law enforcement. *Recommendations to expedite the Bureau's buildout and ensure that it has a clear mandate to coordinate strategy on the full range of emerging technology issues, in addition to critical cybersecurity needs, can be found in the Chapter 15 Blueprint for Action.*
- **Strengthen the U.S. Government's ability to take down botnets by enacting Section 4 of the International Cybercrime Prevention Act.[25]**

- Botnets are already a present threat, and may become more powerful with advances in AI, not just directly spreading malware, but harvesting both computational power and data to put toward further offensive training in ways that were not previously possible. To enable the U.S. Government to better work with private industry and international partners, Congress, in consultation with the Department of Justice, should enact Section 4 of the International Cybercrime Prevention Act.[26] This legislation would provide broader authority to disrupt all types of illegal botnets, not just those used in fraud.[27]

Actions for Cyber Command, the Department of Homeland Security, the Federal Bureau of Investigation, and the National Security Agency:

- **Expand current cyber threat inoculation initiatives.**
  - Machine speed information sharing is a key piece of enabling AI-cyber defenses. To contribute to the readiness of U.S. defense and critical infrastructure, efforts should be made to accelerate sharing of the most recent malicious code captured in the wild through appropriate interagency channels, including through a Joint Collaborative Environment. U.S. Cyber Command should ensure and accelerate coordination with DHS, the FBI, NSA, and stakeholders in the private sector in the release of threat information, particularly with owners and operators of systemically important critical infrastructure.[28]

Section 4: Coordinating and Strategizing a Response.

Recommendation

Recommendation: Reform the U.S. Government's strategy, structure, organization, and authorities for handling AI-enabled cyber threats.

The U.S. must organize and align authorities to fully implement the cyber security mission and fully capitalize on machine speed information sharing defenses. Technology alone isn't enough: Cyber threat intelligence, joint planning, and response must be integrated into the same organization to keep pace with AI cyber threats.

Actions for the Executive Branch:

- **Issue an updated National Cyber Strategy with the following components.**
  - First, the strategy should build on the layered deterrence framework put forward by the Cyberspace Solarium Commission with a focus on making the framework more robust against the ways AI will transform cyber conflict.[29]
    - To support the strategy, the Department of Defense, in partnership with the Department of State and the IC, should also develop a multitiered signaling strategy and promulgate a declaratory policy that addresses the use of AI in cyber operations.[30]
  - Second, to inform the strategy, the Department of Homeland Security should run a study to develop regulatory recommendations for the most cost-effective means of defending digital devices and infrastructure. This study should investigate, but not be limited to:

- Standards requiring critical private and public sector networks to keep their data encrypted at rest and in transit
- Multifactor authentication requirements for critical private and public sector networks
- Air gapping requirements for select sensitive, but still unclassified, networks
- Analog defenses for cyber physical infrastructure to prevent the most lethal failures regardless of how much network access cyber attackers gain, or how advanced their methods of attack become
- Federated machine learning techniques that lower espionage and privacy risk via enabling data to be partitioned or remain decentralized
- Specialized, narrow purpose computation hardware that can't be repurposed by malware for attacks
- Ways to harness AI to lock down and constrain hardware toward its intended purpose on vulnerable networks that can't yet be patched or replaced
- Ways to use cloud computing and virtual machines to reduce vulnerability of AI and cyber systems to advanced persistent threats

- **Accelerate the establishment of a Joint Cyber Planning and Operations Center, modeled after the National Counterterrorism Center.**[31]
  - This planning office under the Cybersecurity and Infrastructure Security Agency is necessary to coordinate cybersecurity planning and readiness across the federal government and between public and private sectors. To properly stand-up such a collaborative environment, the Executive branch must submit to Congress a list of authorities and data sharing issues that will require additional authorities or funding.
- **Develop and implement an information and communications technology industrial base strategy.**[32]
  - This strategy must increase support to supply chain risk management efforts, and provide better defense to the hardware supply chains, data, and algorithms that compose the "AI stack."

Action for Congress:

- **Establish a Bureau of Cyber Statistics to inform both cyber defense policy and AI-enabled cyber defenses.**[33]
  - Large accurate data sets with relevant data are especially useful for training AI-enabled cyber defenses that minimize the costs of cyber attacks and false alarms, rather than just the number of attacks and false alarms. To that end, Congress should establish a Bureau of Cyber Statistics, within the Department of Commerce, or another department or agency, that would act as the government statistical agency that collects, processes, analyzes, and disseminates essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other federal agencies, state and local governments, and the private sector.[34]

Recommendation

Recommendation: Coordinate with the Private Sector to Increase Resilience Against AI-Enabled Cyber Attacks.

Action for Congress:

- **Create or Designate Critical Technology Security Centers.**[35]
    - Congress should direct and appropriate funding for the Department of Homeland Security, in partnership with the Department of Commerce, Department of Energy, Office of the Director of National Intelligence, and Department of Defense, to competitively select, designate, and fund up to three Critical Technology Security Centers.
    - These Centers would be designed to centralize efforts directed toward evaluating and testing the security of devices and technologies that underpin our networks and critical infrastructure.

- **Authorize, establish, and fund a joint collaborative environment for sharing and fusing threat information.[36]**
    - Sharing and fusing threat information is an instrumental step in improving the speed and capability of potential AI-enabled cyber defenses.[37] Congress must ensure that Executive branch agencies have necessary authorities to bring their data together in support of these efforts. Likewise, Congress must create incentives—including liability protection—to attract the private sector to participate in threat information sharing programs.
    - To achieve these goals, the Commission endorses the Cyberspace Solarium Commission recommendation for Congress to establish a 'Joint Collaborative Environment,' a common, cloud-based environment in which the federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis—to the greatest extent possible.[38]

Blueprint for Action: Chapter 1 - Endnotes

[1] For the purposes of this section, "malign information" includes both disinformation—false information or intentionally misleading facts communicated with the intent to deceive—and misinformation—false information not necessarily meant to deceive. See Daniel Fried & Alina Polyakova, *Democratic Defense Against Disinformation*, Atlantic Council at n.1 (Feb. 2018); https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf. For a broader discussion, see Laura Rosenberger, *Making Cyberspace Safe for Democracy*, Foreign Affairs (May/June 2020), http://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy. For a study of how AI might be used to counter disinformation, see William Marcellino, et al., *Human-machine Detection of Online-based Malign Information*, RAND Europe (2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA519-1/RAND_RRA519-1.pdf.

[2] *National Security Strategy of the United States*, The White House at 34 (Dec. 18, 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

[3] Pub. L. 116-92, The National Defense Authorization Act for FY2020, 133 Stat. 1198, 2129-30 (2019).

[4] *National Counterintelligence and Security Center*, Office of the Director of National Intelligence (last accessed Feb. 8, 2020), https://www.dni.gov/index.php/ncsc-home.

[5] *About*, Global Internet Forum to Counter Terrorism (last accessed Oct. 2, 2020), https://www.gifct.org/about/.

[6] Press Release, Office of the Director of National Intelligence, *Director of National Intelligence Daniel R. Coats Establishes Intelligence Community Election Threats Executive*, (July 19, 2019), http://www.dni.gov/index.php/newsroom/press-releases/item/2023-director-of-national-intelligence-daniel-r-coats-establishes-intelligence-community-election-threats-executive.

[7] Brett McGurk, *America Should Build an International Coalition Now*, The Atlantic (March 29, 2020), https://www.theatlantic.com/ideas/archive/2020/03/america-should-build-international-coalition-now/608983/.

[8] Though this overall Blueprint for Action uses the term "malign information" to broaden beyond disinformation to include misinformation, it will likely be easier to organize a task force around countering disinformation.

[9] Funding level should depend upon the number of programs DARPA has the capacity to execute in this area.

[10] See, e.g., Paul England, et al., *AMP: Authentication of Media via Provenance*, arXiv (June 20, 2020), https://arxiv.org/abs/2001.07886.

[11] See *Creating the Standard for Digital Content Attribution*, Content Authenticity Initiative (last accessed Feb. 19, 2020), https://contentauthenticity.org/; *Overview*, Project Origin (last accessed Feb. 19, 2021), http://www.originproject.info/about.

[12] These could be SBIRs, OTAs, or other modern vehicles with minimal red tape. Recently published reports on countering malign influence have issued wide-ranging recommendations including: deploying special operations forces to areas "vulnerable to political warfare," building "rapid-reaction information cells to track and counter" malign influence operations, and promoting civil society to "combine the values of accurate media with engagement skills and an understanding of how propagandists prey on polarization, inflaming divides." These recommendations are already being put into action by Special Operations Command in Africa, using commercially available services to combat and attribute malign information operations about COVID-19 and other issues on the continent. The General Services Administration has awarded IST Research a Phase III SBIR contract to "support operations in the information environment for the special operations and Federal Government community." Additionally, the U.S. Air Force and U.S. Special Operations Command have contracted with Primer to "automatically identify and assess suspected disinformation" using ML technology. See David Ronfeldt & John Arquilla, *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft*, RAND at 72 (July 2020), https://www.rand.org/content/dam/rand/pubs/perspectives/PEA200/PEA237-1/RAND_PEA237-1.pdf (citing or quoting other experts or reports); Dave Nyczepir, *SOCOM Looks to Combat Disinformation in Africa on New Governmentwide Contract*, FedScoop (July 27, 2020), https://www.fedscoop.com/socafrica-disinformation-ist-research/; *IST Research Awarded Five-year, $66 Million GSA Contract*, IST Research (July 23, 2020), http://www.

globenewswire.com/news-release/2020/07/23/2066650/0/en/IST-Research-Awarded-Five-year-66-Million-GSA-Contract.html; *SOCOM and US Air Force Enlist Primer to Combat Disinformation*, Cision PR Newswire (Oct. 1, 2020), https://www.prnewswire.com/news-releases/socom-and-us-air-force-enlist-primer-to-combat-disinformation-301143716.html.

[13] Nicholas Duran, et al., *2018 Webroot Threat Report*, Webroot (2018), https://www-cdn.webroot.com/9315/2354/6488/2018-Webroot-Threat-Report_US-ONLINE.pdf; Gary J. Saavedra, et al., *A Review of Machine Learning Applications in Fuzzing*, arXiv (Oct. 9, 2019), https://arxiv.org/pdf/1906.11133.pdf; Isao Takaesu, *Machine Learning Security: Deep Exploit*, GitHub (Aug. 29, 2019), https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit; Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, Wall Street Journal (Aug. 30, 2019), https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402; *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine (2019), https://doi.org/10.17226/25488; Ben Buchanan, et al., *Automating Cyber Attacks: Hype and Reality*, Center for Security and Emerging Technology (Nov. 2020), https://cset.georgetown.edu/research/automating-cyber-attacks/; Nektaria Kaloudi & Jingyue Li, *The AI-Based Cyber Threat Landscape*, ACM Computing Surveys at 1-34 (Feb. 2020), https://dl.acm.org/doi/abs/10.1145/3372823; Dakota Cary & Daniel Cebul, *Destructive Cyber Operations and Machine Learning*, Center for Security and Emerging Technology at 5-23 (Nov. 2020), https://cset.georgetown.edu/research/destructive-cyber-operations-and-machine-learning/.

[14] Max Heinemeyer, *Dissecting the SolarWinds Hack without the Use of Signatures*, Darktrace (Jan. 7, 2021), http://www.darktrace.com/en/blog/dissecting-the-solar-winds-hack-without-the-use-of-signatures/.

[15] See *EINSTEIN*, U.S. Cybersecurity & Infrastructure Security Agency (last accessed Feb. 8, 2021), https://www.cisa.gov/einstein.

[16] Gregory C. Wilshusen, *DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks*. Government Accountability Office, (April 24, 2018), http://www.gao.gov/assets/700/691439.pdf. See also *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, Government Accountability Office (Jan. 28, 2016), https://www.gao.gov/assets/680/674829.pdf.

[17] *President's FY 2021 Budget Request to Congress for the National Institute of Standards and Technology*, National Institute of Standards and Technology (2020), http://www.nist.gov/system/files/documents/2020/02/11/FY2021-NIST-Budget-Book.pdf.

[18] *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine at 17-19 (2019), https://doi.org/10.17226/25488.

[19] *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine at 12-19 (2019), https://doi.org/10.17226/25488.

[20] *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine at 15 (2019), https://doi.org/10.17226/25488.

[21] *Report*, U.S. Cyberspace Solarium Commission (March 2020), https://www.solarium.gov/report. [*hereinafter* CSC Report]

[22] This recommendation modifies an existing Cyberspace Solarium Commission recommendation in order to reduce the risk of creating perverse incentives to avoid enforcement. See recommendation 4.2 and 4.4.4, CSC Report at 76, 83.

[23] See recommendation 4.4.4, CSC Report at 83.

[24] See recommendation 4.4.3, CSC Report at 82.

[25] See recommendation 4.5.3, CSC Report at 87.

[26] S. 3288, International Cybercrime Prevention Act of 2018, 115th Congress (2018), https://www.congress.gov/bill/115th-congress/senate-bill/3288/text.

Blueprint for Action: Chapter 1 - Endnotes

[27] *Report of the Attorney General's Cyber Digital Task Force*, U.S. Department of Justice at 124 (July 2, 2018), https://www.justice.gov/archives/ag/page/file/1076696/download.

[28] See recommendation 6.1.2, CSC Report at 114.

[29] See recommendation 1.1, CSC Report at 32.

[30] See recommendations 1.1.1 and 1.1.2, CSC Report at 32.

[31] See recommendation 5.4, CSC Report at 87.

[32] See recommendation 4.6, CSC Report at 88.

[33] See recommendation 4.3, CSC Report at 78.

[34] CSC Report, 78.

[35] See recommendation 4.1.1, CSC Report at 75.

[36] See recommendation 5.2, CSC Report at 101.

[37] The President's National Infrastructure Advisory Council detailed a similar recommendation to make cyber intelligence more actionable. *Transforming the U.S. Cyber Threat Partnership*, President's National Infrastructure Advisory Council at 8 (Dec. 12, 2019), https://www.cisa.gov/sites/default/files/publications/NIAC-Working-Group-Report-DRAFT-508.pdf.

[38] CSC Report at 102