MEMORANDUM FOR SCUSA 72

SUBJECT: The United States & the Political Economy of Innovation, Disruptive Technology and American Influence in the Coming Decade

1. **Mission Understanding:** To secure America’s future, we must be first in global innovation. This pertains to select technology areas expected to cause disruptions to world order, including artificial intelligence, quantum computing, synthetic biology, and advanced cyber weapons. Failure will limit opportunities for our future, and establish international norms reflecting our competitors' interests. We must foster an environment friendly to innovation, while defending citizen's privacy. The five areas we must target to succeed are: the education system, industry staffing, communication with the public and private sectors, and regulating the technology and security industries. Leading in innovative technology will encourage our allies and competing countries to emulate our values as they recognize the benefits that democracy provides.

Through the next 10 years, success and failure of this mission can be defined through:

   a) Response time to cyber attacks
   b) The trade deficit in advanced technology goods
   c) The number of new technologies created in the United States vs. abroad
   d) Talent retention; university level and above

2. **Education System:** To address the knowledge and expertise gaps in the education system, we recommend:

   a) Increasing enrollment and graduation of cybersecurity professionals from public higher education institutions
   b) Introducing technology proficiency classes in mandatory education
   c) Subsidizing education costs for students attending public universities pursuing cybersecurity degrees
   d) Funding to be designated by the Secretary of Education and Congress to allocate funds for:
I. Students studying for various cybersecurity certificates

II. Students attending higher education for cybersecurity degrees

III. Implementing experts to generate technology proficiency curriculum to include in mandatory education
   
   e) Collaborate with public universities to establish:
      
      I. Cybersecurity courses and programs
      II. Funding the education of cybersecurity students

The U.S. will produce graduates with the skills necessary to complete the cybersecurity goals of the U.S. The U.S. must have an informed citizenry prepared for the challenges posed by these disruptive technologies.

2a.) **Partnerships:** Our capitalist system enables inter-company competition to constantly innovate and improve new technologies.

   a) Strengthen workforce between the private and public sectors
   
   b) Encourage talent from the university level
   
   c) Learn transferable skills within the industry
   
   d) Ensure a competitive advantage to strengthen disruptive technology workforce in public and private sectors
   
   e) Create public/private partnerships for individuals beginning participation in this sector at the university level
   
   f) Foster adaptable workforce to public and private initiatives by teaching encompassing curriculum of cyber security skills
   
   g) Promote a system of public/private partnerships with public higher education to:
      
      I. Create new job opportunities
      II. Expand collective knowledge
      III. Develop new national security capabilities
Private companies (i.e., Mastercard and Microsoft) partner with the government to incentivize a transition of public sector cyber security employees to private sector cyber security. This allows for a more innovative workforce in the private sector and promotes communication between the public and private cyber security sectors. Current programs offer up to $75,000 tuition assistance for those in this program. The U.S. government should match private sector financial assistance for students staying in the public sector.

2b.) **Staffing:** To expand the scope of the cybersecurity and data analytics workforce and staffing, we must establish educational programs for incentivizing a wide range of talented individuals to pursue careers in these fields. These programs include:

   a) Improved communication between employers and universities to ensure the quality of technical skills

   b) Accelerated courses (i.e., DARPA CS program) to universities and colleges

   c) Trade schools and programs concentrating on computer science certifications

   d) Partnered educational programs by the private sector (i.e., programs by Microsoft or Google)

   e) Implementation of a federal database listing STEM opportunities for staffing, research, continued-education programs, advisors/mentors, and returning or nontraditional student programs

   f) Incentivizing returning and non-traditional to join the STEM workforces to fill market demand and expand the STEM sector by expanding federal student loan forgiveness programs

   g) Web Accessibility Initiative partnerships

3. **Regulations:** In our pursuit of innovating technologies to promote U.S. values abroad, we cannot neglect the liberties of American citizens. Regulation policies are categorized domestically or internationally.

   a) Domestic:

      I. Private platforms must offer comprehensive notification of the risks or benefits of collecting personal data, including data harvesting
II. Require terms and conditions of use written in simple language

III. Communicate risk in using a platform

IV. Encourage choices between subscription-based service-us of their services or comparable alternatives to data harvesting as compensation.

V. Borrow ideas from the EU’s General Data Protection Regulation (GDPR)

VI. Allow for fast-tracked research/testing areas and the opportunity to test technologies in highly secure and regulated environments

b) International:

I. Emphasize U.S. security with new and emerging technology

II. Implement a non-compete clause for new Ips

III. Any international film by foreign government controlling more than 10% equity stake must report data collection and file a statement of intent in U.S.

IV. All films operating in the United States must mandate self-reporting of data breaches affecting more than 1% U.S. customers and communicate the steps taken to reduce this risk

V. The goal of regulation is to drive innovation. This must not come at the cost of the liberties of American citizens. Conversely, elevating the protection of Americans over the necessity of innovation would be detrimental to the development of technologies vital to U.S. competitiveness

4. Security: We seek to deter and deny cyber-attacks on infrastructure, through offensive and defensive measures. As we compete with China to develop and integrate emerging technologies, we must establish resiliency and resistance in our critical infrastructure to ensure an environment in which these innovations can occur.

a) Defensively:

I. Incentivize private companies within these industries to meet standards of security and cybersecurity

II. Provide tax incentives for complying with benchmarks of security standards
The U.S. Securities and Exchange Commission (SEC) should assess companies' security, a metric to disclose to shareholders.

Fund U.S. Cyber Command Joint Cyber Warfighting Architecture (JWCA) to develop a defense strategy.

Share security intelligence across borders with allied nations who can help defend against where cyber-attacks are underway.

Adequate funding must be allocated to the JCWA and the FBI to increase capability of policing cyber criminals.

A preliminary stand-by period of 2-5 years (depending on industry) for companies to integrate new security measures in accordance with the guidelines of the tax incentive and SEC.

The point of contact for this memorandum is CDT SGT Grant Nawoichyk at grant.nawoichyk@westpoint.edu or 845-235-6963.

The United States & the Political Economy of Innovation Table
The United States & the Political Economy of Innovation
SCUSA 72
United States Military Academy