

GLOBSEC GeoTech Center Dinner Roundtable: Exploring the Nexus of Tech and National Security under the Incoming Administration

2nd December, Washington DC

Context:

Nearly every dimension of geopolitics and the global geostrategic relationships in the 21st Century will be shaped in some form or fashion by both advances in tech, and these advances will in turn be shaped by the speed with which tech is evolving. The new Trump administration will have to face all these realities, realities that so much has changed so dramatically while Donald Trump was out of office that some of these technologies are virtually unrecognizable from where they were just four years.

How should the incoming administration think about foreign policy that is informed and, in many respects, is driven by evolving technologies and the inevitable global tech competition? What are the key critical areas that will be prioritized by the new administration? How should the U.S. redefine its relations with key partners globally – from European allies to allies in the Indo-Pacific region – in order to not only support economic growth but also counterbalance the influence of China’s expanding digital presence globally?

Key takeaways:

Strategic Challenges and Solutions for the New Administration

- **Technological Edge:** Securing our technological edge is critical to addressing challenges from nations like China, Russia, and Iran. This is a matter of national security, demanding lessons from history and current events. No single entity can manage this alone; gaps and indecision will create vulnerabilities. Unified, decisive action is imperative.
- **Authoritarian vs. Democratic Innovation:** Authoritarian governments, such as those in China and Russia, often excel in leveraging technology effectively due to their ability to act decisively and direct innovation toward state objectives. Because there’s virtually no separation between the governments and the “private sector”, these regimes impose mandates on their tech sectors to serve strategic goals, enabling them to harness advancements and move to application efficiently. In contrast, democratic governments, despite possessing some of the world's best technology, often struggle to fully utilize and integrate their innovations due to systemic constraints and inefficiencies. Consequently, democracies may find themselves at a technological disadvantage—not because of a lack of innovation, but because of onerous regulatory constraints, and challenges in mobilizing and aligning their advancements.
- **Non-Kinetic Warfare:** Shift from Kinetic to Non-Kinetic Warfare: While the Westphalian, state-centric system will still dominate state to state relationships, technology is increasingly being used as a more effective means of advancing state interests than traditional military actions (kinetic warfare). Russia's actions in the cyber and information domains, aimed at undermining Ukraine’s fledgling democracy and Russia’s and China’s direct interference in governance and in the societies of other countries, particularly democracies, through non-kinetic means, illustrate this shift.
- **Big Tech's Role:** Large tech companies have significant resources, global reach, and expertise, making them uniquely capable of addressing complex technological challenges. Their appearance on the world stage can both complement and compromise the state-centric system of international relations. As these private sector entities increase their global influence there will inevitably be adjustments to the system of international relations. Whether or not these adjustments favor the international rules-based system remains to be determined.

Technological Innovation and Speed

When considering technological innovation and speed, technologies like AI, Quantum Computing, and energy are advancing at an unprecedented pace and unprecedented potential. The United States must heavily invest in research and development to maintain its edge while ensuring these innovations are safeguarded against adversaries. Additionally, securing critical supply chains, such as access to critical materials, rare earths, and semiconductors, is crucial. Collaborating with allies like Taiwan is essential to mitigate strategic vulnerabilities and ensure resilience in the face of global competition.

Public-Private Collaboration

Public-private collaboration is essential for maintaining a competitive edge in defense and intelligence. Streamlining contracting rules will enable agile tech firms and defense startups to contribute directly to national operations. Relying solely on large defense primes risks stifling innovation. Ukraine's success in leveraging commercial technologies, like cloud systems and drones, on the battlefield underscores the importance of integrating private sector innovation with national strategies. Flexibility in this collaboration is key in order to achieve sustainable progress. Currently, the pace of legal review, and slow process of contracting are major hurdles to the rapid fielding of technologies which, in turn, has a direct and negative impact on national security.

Hybrid Warfare and Security

Ukraine's resilience in the face of Russia's aggression demonstrates the effectiveness of decentralized battle groups and digitized government infrastructure in hybrid warfare. By prioritizing cloud-based systems, for example, Ukrainians ensure continuity during cyber or kinetic attacks. This model offers valuable lessons for modern conflicts.

At the same time, Taiwan's cyber and information vulnerabilities require immediate attention. With daily cyberattacks and hybrid threats from China, including the potential cutting of the undersea cable network into and out of Taiwan, it is critical to assist Taiwan in developing off-island data centers and modernizing its cybersecurity systems. These actions are not just strategic for Taiwan, but are essential to maintaining stability in East Asia, countering emerging threats, and sustaining deterrence across the Taiwan Strait.

Global Partnerships

Global partnerships are necessary for navigating the complexities of today's geopolitical landscape. Collaborating with EU and Indo-Pacific allies through initiatives like the EU-US Trade and Technology Council can help align standards and drive investments in critical areas such as AI, semiconductors, and cybersecurity. At the same time, a unified strategy is needed to counterbalance China's expanding digital presence through its Belt and Road Initiative. By working together to address digital infrastructure and emerging markets, allied nations can ensure a balanced, secure, and sustainable global framework for digital standards and investments into critical infrastructure.

AI Leadership

AI leadership is a cornerstone of maintaining a strategic edge in the tech and geopolitical competition of the 21st Century. To do this the U.S. must scale AI development responsibly while ensuring the energy infrastructure is sufficiently robust to support advanced systems. Virtually none of the existing power grids of the advanced democracies in the world are adequate for the power demands that are coming as emerging technologies continue to scale at breathtaking speeds. Building out these grids, while we are seeking alternative power sources is an essential collaboration going forward. Additionally, collaboration with and among democratic allies, such as the UK and EU, is vital for establishing global AI safety and ethics standards. These efforts are essential to counter the authoritarian misuse of AI and to create a framework that prioritizes responsible innovation, scaling, and shared democratic values.

Balancing High-Tech and Low-Tech Threats

While advanced cyberattacks capture attention, low-tech disruptions, such as sabotage of undersea cables or physical attacks on infrastructure, continue to pose significant risks. Increasing funding to enhance resilience across both cyber and physical domains is imperative. Addressing these vulnerabilities ensures a more comprehensive approach to safeguarding critical infrastructure against evolving threats.

Lessons from Ukraine and Taiwan highlight the importance of prioritizing tangible, actionable projects. Secure data centers, agile defense systems, and digitized government services not only enhance resilience but also gain support from key stakeholders. Focusing on these initiatives ensures practical outcomes while addressing critical vulnerabilities in an increasingly complex security landscape.

Re-examine U.S. Innovation Strategy

The loss of U.S. dominance in 5G to Huawei underscores the need for greater government involvement in aligning private sector capabilities with national priorities. Future strategies must focus on key areas like AI and quantum computing to avoid similar setbacks. Additionally, attracting top global talent is crucial.

Favorable immigration policies and increased investments in STEM education will ensure the U.S. maintains its competitive edge in the rapidly evolving global landscape.

NATO and European Defense Coordination

NATO and European defense coordination must adapt to evolving threats by prioritizing investments in advanced technologies. Encouraging NATO and EU allies to adopt AI, drones, and other innovative defense systems is essential, as demonstrated by Ukraine's resilience. Additionally, enhancing intelligence-sharing mechanisms with European partners is critical to countering shared cyber threats, particularly those posed by Russia and China. These steps will ensure a unified and modernized approach to collective security.

Recommendations for Implementation:

- **Streamline Defense Contracting:** Allow firms of all sizes to compete along with large defense contractors through fast-track, significantly accelerated procurement programs.
- **Strengthen and Further Secure Supply Chains:** Collaborate with Taiwan, Japan, South Korea, and other strategic partners on semiconductor production while securing critical minerals and rare earths through partnerships with Australia and African nations.
- **Establish AI and Quantum Alliances:** Launch a formal AI-Quantum Security Alliance with the EU, Japan, and South Korea to coordinate Research and Development, safety protocols, and ethical use guidelines.
- **Taiwan Contingency Planning:** Form a dedicated task force with Indo-Pacific and European allies to prepare for potential crises in the Taiwan Strait, emphasizing hybrid and cyber defense readiness.
- **Incentivize Resilience Programs:** Provide support or tax incentives to companies developing secure cloud systems, infrastructure monitoring tools, and hybrid threat defense technologies.