Citizenship Hedging

Mid-future neutral scenario

E-residency is a system originally piloted in Estonia that allows globally itinerant or location-independent business owners and entrepreneurs to avail themselves of certain national services and resources in a foreign country without being a citizen there. As similar programs popped up across the globe, e-residency became a popular method to seek safe haven for companies in potential conflict zones. With mounting problems like political destabilization and climate change, securing e-residency abroad proved a valuable insurance policy for one’s business—or even one’s own well-being. Participating countries allow e-residents to take up physical residence for a limited period of time, if necessary, and while e-residency doesn’t secure citizenship, it can improve your chances of moving up the immigration list. Not a bad option for those who don’t have a bunker in New Zealand to escape to.
5TH YEAR ON THE LIST

Legacy IT Infrastructure

KEY INSIGHT

Parts of the federal government rely on comically old technology, which is very difficult to maintain. However, overhauling the infrastructure has bipartisan appeal.

EXAMPLES

In 2020, millions of people tried to file unemployment claims, and registration systems in 19 states crashed under the stress. Many systems haven’t been updated since they were built in the 1980s. A desperate New Jersey Gov. Phil Murphy held a press conference pleading for volunteer COBOL programmers to help fix the state’s automated benefits system. It took five months to issue $1,200 stimulus checks to eligible taxpayers because the Internal Revenue Service computer systems, built in the 1970s, couldn’t be easily reconfigured. The U.S. government wastes $80 billion each year due to obsolete technologies and inefficiencies, according to a 2016 U.S. Government Accountability Office report. That sobering tech audit found that the State Department tracks visa information for 55,000 foreign nationals using a 26-year-old system that’s been decommissioned by the software maker.

DISRUPTIVE IMPACT

Fixing legacy systems is a technological as well as cultural challenge. Upgrading a legacy system that’s critical for day-to-day operations would cause major disruption, and government offices, already strapped for personnel, don’t have easy workarounds. And because the systems are taxpayer funded, government agencies tend to underinvest, avoid maintenance, and cut corners on upgrades to save money. Few technicians have enough institutional knowledge to make the necessary fixes, which means rehiring retired employees at high contract wages. Legacy systems are also vulnerable to attack.

EMERGING PLAYERS

• U.S. Government Accountability Office
• United States Digital Service
• Office of Management and Budget
• Office of Science and Technology Policy
2ND YEAR ON THE LIST

China’s Quest for Cyber Sovereignty

KEY INSIGHT

Cybersovereignty refers to a government exerting control over how the internet is run, who gets access to it, and what can be done with all of the data generated.

EXAMPLES

In 2019, Chinese President Xi Jinping pushed forward an agenda of strict control, censorship, and suppression, and the country began exporting its systems to authoritarian leaders elsewhere in the world. And last year, provocative crackdowns on Hong Kong by the Chinese Communist Party (CCP) resulted in an expansion of China’s Great Firewall, a tightly controlled version of the internet that blocks entertainment, journalism, and commentary that challenge the government’s ideas. In January 2021, the CCP announced plans to nationalize Alibaba and Ant Group, two of China’s most successful big tech companies.

DISRUPTIVE IMPACT

The CCP argues that China is an enormous country in the midst of the fastest economic transition in modern history, and its unique controls promote social and economic stability. But there’s more to it than that: In 2019, Xi also announced that the government would wean itself off foreign-made computers and operating systems, replacing familiar brands (Microsoft, Dell, Apple) with Chinese products. Xi has said China’s digital and information systems can serve as a new model for other countries around the world and that other authoritarian regimes can follow suit. China’s Belt and Road Initiative, which has successfully expanded trade throughout emerging economies, has boosted the country’s digital initiatives. Within a decade, the digital world could be split in two: a free system in the West and a closed system led by China.

EMERGING PLAYERS

• Ant Group
• Alipay
• ByteDance
• Ren Zhengfei, Huawei founder
• Lei Jun, Xiaomi founder
• Pony Ma, Tencent founder
• Liu Chuanzhi, Lenovo founder
• Jack Ma, Alibaba founder

Chinese President Xi Jinping wants his country to be technologically independent this decade.
The U.S. Defense and Space Future Will Require Flexibility and Adaptability

Lt. Col. Jake Sotiriadis, Ph.D.
Strategic Foresight and Futures Branch Chief
Headquarters, US Air Force

In 2021, a cycle of rapid change, growing complexity, and radical uncertainty will intensify the urgency for the national security establishment to become more adaptable to the unexpected. The COVID-19 pandemic revealed overlooked vulnerabilities for supply chains, our society, our economy, and our national security strategy.

The new strategic environment affects many of the baseline assumptions that underpin our national security strategy and service-level warfighting concepts. In light of these challenges, how can defense planners mitigate uncertainty?

Strategic foresight and futures thinking can lend insights into sources of disruption and disruptive technologies, by harnessing environmental scanning, weak signals, and emerging trend analysis. The security landscape of a post-Covid world contains both challenges and opportunities that will continue to defy accepted probabilities in defense.
This includes the definition of what constitutes national security itself, which today must encompass non-traditional items, such as bio-security and advances in CRISPR technology. Signals and trends today also point to future developments in anticipatory health platforms that will be powered by quantum processors.

In 2021, disinformation is no longer limited exclusively to Russia, China, Iran, or violent extremist organizations. Rather, we are likely to see these actors waging simultaneous, multi-faceted influence campaigns on targeted populations at a global scale. These campaigns will continue to target all facets of our society.

We can expect to see increased defense partnerships with the technology sector—with traditional social media platforms as well as with startups developing emerging platforms to identify disinformation patterns. As we continue to focus on the competition among great world powers—with China and Russia as the primary threats to U.S. security—we also cannot lose sight of the new, emerging fault lines in the Middle East or complex crises on Europe’s periphery.

Covid’s disruption has also accelerated the export of China’s worst characteristics, while prompting delays and disruptions to the country’s Belt and Road Initiative. In the U.S. homeland, overly thin levels of inventory and long supply chains present risks to national security. The second and third order effects of Covid also increase the potential for more surveillance and automation in the name of public health—much as the terrorist attacks on Sept. 11, 2001, did for airport security procedures.

In the space domain, expect a targeted set of strategies to ensure the immense progress made in the commercial space industry over the past two decades is not lost. The need to accelerate space programs and transform capabilities in a fiscally constrained environment will feed investment in a technology pipeline, spur agile contracting, and strengthen partnerships with the commercial sector and international partners. This approach will alleviate weak supply chains, leverage cutting-edge technologies, and strengthen gaps in areas that require international cooperation (such as debris mitigation, space traffic control, and behavioral norms).

Military and national security entities will be consumed with networking their forces and trading information and data. This means moving toward cloud-based solutions that enable instantaneous
Here, we refer to a disciplined way of:

1. Questioning our assumptions
2. Seeing the interconnectivity of events
3. Embracing analytic complexity in our strategic planning

Doing so requires both crafting and proliferating better methodologies for anticipatory thinking.

Digital solutions are necessary—but not sufficient—for success in retaining decision advantage. Seizing and occupying the cognitive high ground in the national security arena means more than just “buying things,” developing weapons systems, or increasing technological leverage. It means also ensuring that professionals are given powerful technological tools with the requisite cognitive capacity for sense-making.

Last year was a critical one for digital transformation across all sectors, but make no mistake—2021 will be a year when companies seek increasingly innovative means to derive value chains from technology. It will be a year in which intentional strategies are indispensable to achieving success. In national security, defense, and the corporate world, organizations cannot simply “stumble” into tech solutions (as was the case in many instances in 2020). Absent a deliberate strategy and a clear road map for implementation, even the most advanced or disruptive technologies will not be a panacea.

Maximizing human capital will require creating, enhancing, and developing our cognitive operating system.

Lt. Col. Jake Sotiriadis, Ph.D., is the U.S. Air Force’s senior futurist. His work spans the nexus of disruptive technology, geopolitical risk analysis, intelligence, and alternative futures. He leads a team that helps senior leaders in the Department of Defense and the Intelligence Community develop anticipatory thinking and conceptualize breakthrough innovations. He holds a Ph.D. in political science from the University of Hawai’i at Manoa and master’s degrees from the Fletcher School of Law and Diplomacy at Tufts University, the School of Advanced Air and Space Studies, and the Air Command and Staff College.

The views expressed in this section are those of the author and do not reflect official positions or endorsements of the U.S. Air Force or the Department of Defense.