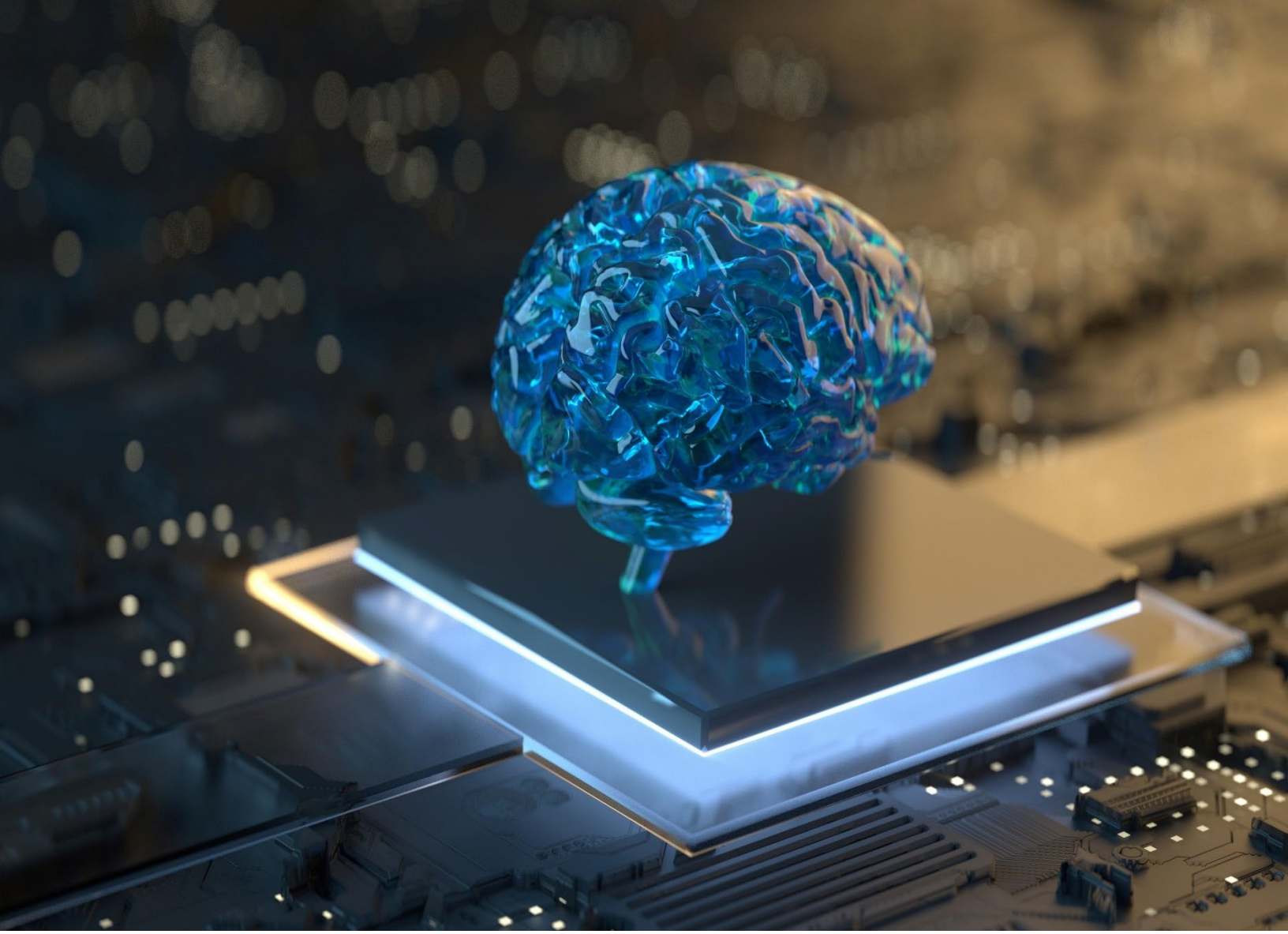

Preparedness in Times of Rapid Change

July 2023

Science and Technology

CONTENTS

Introduction

In ways not experienced in every generation, the world is entering an uncommon period of transformational change that will have implications on how we protect the homeland. To a large extent, there is no context or historical reference for how this change will impact society for the here and now and over the horizon. The exponential growth of advanced technologies, rapid innovation shaping the marketplace of ideas,[1] a changing outlook on the future as well as the essence of the great power competition are all underlying drivers. Additionally, extreme weather variations and large environmental shifts, all against the backdrop of large-scale geopolitical realignments, impact the context and intent of our actions. Our ability to safeguard the American people, our homeland, and our values must be attended to today. We must take full advantage of current technological development, but at the same time, recognize that the world of tomorrow may be vastly different with future challenges that may not easily scale from where we are today. On the cusp of this new frontier, we must hedge against and be prepared for what are likely not simple extensions of where we are today.[2]

A Changing Landscape

Emerging technologies today are evolving in many unexpected ways. These technologies span dozens of domains, including advanced manufacturing, nanomaterials, autonomous systems, genomic editing and biotechnologies, quantum information science and engineering, generative artificial intelligence (AI), and enabling next generation networks. Many of these are becoming increasingly democratized,[3] which we define to be much more than just greater ease of use. Specifically, this is meant to include the effects of commercial markets making technologies cheaper, more capable, and faster to implement—and thus lowering the threshold for use. But what is more important is the ensuing empowerment of users to immediately create novel products and platforms. Open innovation due to global connectivity spreads and accelerates innovation allowing essentially anybody to participate. Empowerment is dependent on factors such as connectivity of the users, affordability, and accessibility of tools as some of the enablers. The development of these as technology platforms serve to increase accessibility, blend technologies together to further invent, reduce cost, and help draw in more fast followers and co-innovators. In turn, empowered actors, limited only by their creativity, can bring about the unexpected at low cost but with disruptive consequences. This dynamic is not readily bounded by borders and the global scale is evident in how this is unfolding today. Many of these emerging technologies bring about deep questions on how to impose ethical standards, how to develop overarching regulatory structures, or whether to push for the

[1] For instance, consider the explosive growth of large language models, foundation models, and generative AI, that is fostering a rich diversity of novel use cases that span economic sectors, also accompanied by adversarial threats that include concerns about the undermining of democratic institutions, transnational repression, or other forms of influence operations. In this context, the marketplace of ideas is not a marketplace for norms or adequate consideration of societal impacts—these are lagging. This is leading to a new suite of realities and disruptions, which society must be equipped to address.

[2] Many factors will help drive preparedness: driving open standards and greater ability to adapt/build-on existing technologies for changing environments; working across the diverse homeland security missions to increase the scale of common underlying needs; thinking beyond technology horizons where limited market forces exist to meet otherwise boutique needs; working with the private sector more deeply to augment their R&D roadmaps, cobble together disparate pockets of innovation with adequate intellectual property (IP) considerations, create a richer ecosystem of performers and solutions that can add needed functionality for homeland security missions. The ability to pivot will need flexibilities in operating within top line appropriations, broadening of the reach of enablers such as the Support Anti-Terrorism by Fostering Effective Technologies, or SAFETY, Act (https://www.dhs.gov/science-and-technology/safety-act), for anti-terrorism technologies and use of Other Transaction Authorities, together with leveraging interagency and international partners.

[3] D. Kusnezov, W.B. Jones, "Are Some Technologies Beyond Regulatory Regimes?" SAND-2017-9186J (2017): https://doi.org/10.48550/arXiv.1707.06668. For democratized technologies, the need for non-traditional approaches to governing/regulating present unique differences to traditional transformational technologies such as nuclear. From the point of view of multiplayer (behavioral) game theory, with many technology users who could have various motivations, the behaviors are shown to be generally chaotic, without Nash equilibria, leading to consideration that far different approaches to managing risks are needed.

development of norms and other international standards or agreements. Generative AI is just a current example of opportunities and risks that surface from democratization.

Against this dramatic absorption of emerging technologies into our lives and environments with their intended and unintended consequences, the world around us is independently experiencing changes and displaying the effects. The Arctic and Alaska are sensitive indicators of this change and offer a unique glimpse into the future. For the United States, the opening of the northern latitudes will have complex geopolitical consequences for protecting borders and waterways, patrol and rescue operations, communications, territorial and resource claims, and the resilience of critical infrastructures. Globally, many factors could be at play that make human habitation challenging in austere environments. These external pressures may result in changing patterns to migration. Emerging technologies and environmental changes bookend the largescale and long-term drivers that require reflection on how to appropriately prepare.

Today, a cadence of extreme weather events continues to surface many secondary and tertiary effects, such as the fragility of existing networks we rely on—transportation, supply chains, or energy distribution, and further downstream consequences that could all be better mitigated through combinations of real-time awareness and prediction. While not driven by emerging technologies, there is a role for these advances to help manage or anticipate the impacts of future change (in the context of preparedness). Already today for well-defined events, pre- and post- event efforts can be enhanced with smarter integrated tools.[4] This will play a role in how we balance resilience versus adaption and adaptation—separating where technology enhanced foresight can help from where new approaches could be considered. The new baseline of such normalcy impacts first responders and emergency managers who face new and unexpected conditions not experientially rooted, which now also span impacts from lithium-ion thermal runaway fires to generative AI. While the precise unfolding of events is uncertain, what is clear is that our sense of preparedness should be appropriately inclusive of such considerations—driven by both natural and human induced change. Balancing the promises of technology with the impacts and opportunities for the changing world is a key concern for government and industry alike. How we arrive at that balance and understand what these challenges mean for adaptation and security, is explored below.

Beyond Incrementalism: The Role of Science and Technology in this New Space

Solutions to the challenges we face require a balance of policy, human capital, and technology. Current approaches are evolutionarily connected to how we addressed problems historically, often with models of risk built upon assumptions of incremental changes to the threat environment. Tools, methods, and means have been made more efficient and processes refined to be responsive to increasingly growing demands. The ability of this chosen path to meet future needs underpins our current state of preparedness.

If the future holds only episodic excursions from our current risk models—what could be termed a linear world—then surging or adjusting 'on the fly' is a viable methodology for government response efforts. However, if the future deviates significantly from past experiences, such an approach could be problematic at many levels.

[4] For pre-event, this includes concepts like digital twins, that combine model-based predictions of forthcoming risks—e.g., cloud-to-ground lightning probabilities coupled to fuel loading of the environment—that can help with pre-staging equipment. For post-event, higher sensitivity and targeted environmental sensors for wildfires or floods, broader alerts, warning and notifications, next-generation 911 and emergency operations centers, are among considerations.

Therefore, it is reasonable to ask whether we are in a moment of linear change, or on the precipice of a major inflection. In times of linear change, our risk models are sound, and incrementalism provides for effective enhancements of capabilities. Additionally, natural market developments result in improved and more efficient products, enhancements of existing methods and means, and how we approach the risks of emerging technologies, are adequate. Consequently, we would expect the future of the homeland security mission space to be addressable within the existing approaches, necessitating small adjustments only when deviations from the baseline occur. However, in a non-linear world, characterized by disruption and ambiguity, incrementalism may leave the homeland unprepared.

One of the roles of the science and technology community is to question whether we are in a linear or non-linear world, and whether we are investing appropriately for the future. As the threats have evolved in recent years, the historical distinction between homeland and national security challenges has continued to blur and the role of DHS has grown accordingly.[5] Sharpening our understanding of the current state helps clarify potential futures and surface viable pathways that establish a posture of preparedness. How to prioritize against myriad possibilities and knowing what to change or what the realm of possibilities and options are, requires an understanding of the impacts. For example, whether it's the importance of understanding the impacts of adversarial AI on ever smarter and interlinked cities and lives, impacts of climate driven or gene-edited causes of new patterns and behaviors in disease impacting people, animals or agriculture, or better awareness of how to pre-stage for the more common extreme weather events, science is a tool to understand potential futures and technology is a means to provide nearer term options to mitigate and ideally relieve stress on otherwise overburdened real-time triage. The roles of science and technology are intertwined in establishing this posture, but they are distinct from one another. As Thomas Kuhn wrote,[6] "Scientific development is like Darwinian evolution, a process driven from behind rather than pulled toward some fixed goal towards which it grows ever closer."

The Coevolution of Our Constructs with Technologies

Technology is deeply rooted in how we see the world from how we understand our privacy, our borders, or even facts versus fiction. Perceptions and definitions evolve with technology in nontrivial ways and are confounding factors as we try to be more prepared. Privacy, for instance, has been studied in this context over the years,[7] from the concerns that emerged with the development of the telegraph and telegrams in the mid-1800s, to fears over unauthorized portraiture tied to the development of portable cameras around 1900, to issues of computers, big data, geolocation, third party data brokers, and today's sharing of personal information in disparate dimensions. Technology has forced the reevaluation of the boundaries that were once simpler, forcing nations to update how they govern.[8]

More generally, technologies continue to blur definitions beyond privacy and challenge tested approaches. Our international borders now include a growing virtual component in addition to an ever more complex physical footprint due to technological innovation. This is seen today with how transnational criminal organizations, or TCOs, leverage technology to escape detection, how hackers traffic in software for illicit gain, or pedophiles use technology to engage in child sexual exploitation

[5] DHS Secretary Alejandro Mayorkas, "The Convergence of National Security and Homeland Security," the Center for Strategic and International Studies, (December 2022), Washington, DC, https://www.csis.org/analysis/convergence-national-security-and-homeland-security-conversation-dhs-secretary-alejandro-n.

[6] Thomas Kuhn, "The Trouble with the Historical Philosophy of Science," Department of the History of Science, Harvard University, Cambridge, MA (1992).

[7] See for example, D. Seipp, "The Right to Privacy in Nineteenth Century America," Harvard University (1978), http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf; D. J. Solove, "A Brief History of Information Privacy Law," Proskauer on Privacy, PLI (2006).

[8] Regulation (EU) 2016/679 (General Data Protection Regulation), version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

(CSE). In all these cases, transactions using cryptocurrencies have global reach, providing criminals scale, convenience, and anonymity. For example, a principal mode for CSE has a predator in the United States, a child trafficker in the Philippines together with victims, streaming video on the dark web using air-gapped financial transactions in cryptocurrency. The evolution of the metaverse and its variants provides many ways to influence, to indoctrinate, and to train across borders. Autonomous systems are expanding the physical means to cross land and sea borders that are increasingly more evasive and difficult to detect. Whether by air, sea, or subsurface, the growth in autonomy stresses domain awareness and response.

While watermarking and tool development to establish the provenance of digital content continues to evolve, so does the convenience and sophistication of tools that intermix fact and fiction—not always with malintent. Generative AI is enabling more applications for positive and negative outcomes. "Who are you?" has all new meanings with this technology, and the difficulties in answering this will only grow. Who we are in the world of deepfakes, of morphing, of the endless variations, will add ambiguity to answering what was once a simple question.[9] These issues are amplified at the national level, leading to concerns about transnational repression or foreign driven efforts that can be individually targeted or broadly disseminated toward undermining democratic institutions. At the same time, we are also encouraged today to use technologies to construct our own realities, beyond living in the metaverse. Smartphones have tools that can easily edit people or physical features out of images or add new features, to capture and archive our own versions of our memories and histories. Richer versions of this will emerge in the future. In the evolution from state actors driving revisionism, today's facts and our histories are being changed at all levels of society.

As we watch the dramatic rise of emerging technologies, we must keep in mind how they are not standalone but intertwined with the way we see the world and can shape where it is going in surprising ways.

Innovation Will Be Different: The Need for Technology Artists

Visual artists excel at creating the unexpected with everyday tools. When first taught about colors, we are all introduced to the three primary colors and the wheel they are placed on. We learn to create new colors by mixing, providing a palette that results in complex compositions. Today, emerging technologies are like this visual multimedia. As both democratized and engineering level platforms proliferate, with already many dozens today, the opportunities that arise to blend technologies together to create new operational technologies will not only require fostering non-traditional innovation with the private sector, but it will also make regulating and governing individual technologies more difficult.

As science and technology embraces this convergence, it will drive discovery and invention beyond the boundaries of the traditional disciplines and increase the need for technology artists for the government and society as a whole. As described above, the horizon is more ambiguous than ever. We need more people who can look beyond their traditional training to develop solutions that scale to a constantly evolving homeland security environment, where ideas that lie beyond existing market forces and technology horizons can become high-leverage contributions to those solutions. Whether as an individual, or a member of a team, innovation that fosters the artistry needed for homeland security problems is critical today and for the foreseeable future.

Some of the challenges here lie in innovation being developed in specific IP and technology pockets of specialty. New means that allow ideas across companies to blend to achieve solutions we do not have

[9] DHS S&T Digital Forgeries Report: Technology Landscape Threat Assessment, Report to Congress (January 2023) https://www.dhs.gov/science-and-technology/publication/st-digital-forgeries-report-technology-landscape-threat-assessment.

today are core to a dynamic private sector ecosystem. Smarter ways to intervene and stem the spread of opioids are needed, and there will not be single-point technology solutions. It will take the same artists to shape the world of the possible with the remarkable spectrum of emerging technologies we have today. As these technologies bleed into each other, the challenge of governance becomes more complex in terms of regulating integrated products. For blended technologies—take AI with gene-editing and custom nano-particles manufacturing, or advanced manufacturing for payloads on autonomous drones with quantum-based navigation and AI functionality—regulating a part of a composite system might not impact its growing functionality. Innovations in any of the other technologies could be the enabling mechanisms that lead to overall concerns in their use.

We should not forget to include the need for those in political science, law, anthropology, and ethics when we think about technology artists. Professionals in these disciplines establish the foundation for discovery in our understanding of people and how we come together as a society. Their role in how we will use technologies such as quantum computing, digital identities, and AI will determine success.

With Emerging Technology Comes Emerging Threats

In addition to the positive opportunities provided by emerging technologies, we must also recognize that their use for nefarious purposes will be equally innovative. This dual use has been unfolding for single technologies but is likely to change in character. Today, the challenges in countering unmanned autonomous systems stress our domain awareness and response. For cybersecurity, we have been led to develop incident response centers and means to disseminate best practices, awareness of zero-day or ransomware threats that surface, and response teams to help fix and recover. It is reasonable to anticipate the need for new response centers and teams for capabilities such as adversarial AI or other complex integrated technologies. This will have to be developed in conjunction with technology sector. How we organize around this, with potential broad impacts to societies, does suggest the importance of international partnerships.

While adversarial AI continues to evolve, it is evident the technology will impact the homeland. Already we have observed broad categories of developing attacks, evasion, poisoning, inference, and extraction. Beyond deepfakes today with just video and audio, other modalities will become more common. For those dealing with these on the front lines, working with first responders and emergency operations centers to develop more real-time prediction support is already an existing homeland need. With new kinds of attacks that are hard to trace and mitigate, the roles of first responders are changing. From advanced manufactured skimmers on credit card readers to ghost guns, or AI-based extraction of intellectual property, the opportunities of generative AI to attack, mislead, fool, evade, spoof and so forth, the rapidly evolving landscape of concerns is creating new demand for tools and training for those protecting the front lines.

Some exploits can extract information through model inversion, which has implications for IP or privacy. Traditional cyber malware can be modified with AI to pass through systems undetected. The ability of adversarial AI to target large, interconnected systems, including cities and infrastructure presents new concerns as well. The reality of a massive web of individual devices, networks, and sensors represents security vulnerabilities that can cause harm on an entire system in ways distinct from cyber-attacks.

Beyond deliberate misuses of technologies are concerns where humans are not in decision cycles. This effect was observed in the trillion-dollar, 2010 flash crash of the New York Stock Exchange when high-frequency trading algorithms went awry. We expect advanced systems, composed of blended emerging technologies, to be deployed into lower consequence decision cycles to help manage a world of growing complexity. More exchanges of information at machine speeds and across next generation networks will

make human understanding of functionality, failure modes, or exploits challenging. From unmanned, fully autonomous systems that are not readily intercepted, or quantum computers that can break encryption of current or archived information, or genetically modified diseases—consideration of these is a growing area of significance that must evolve with the technologies.

With respect to the existential risks of AI systems, because they are becoming "intelligent" or providing glimpses of this, it is worth reflecting on what we mean by thinking or how breakthrough scientific ideas germinate. While much can be said here, Heidegger's view is useful:[10] "thinking is not an opinion or notion; it is not having an idea about something; nor is it a sequence of premises that lead to a valid conclusion, nor is it conceptual." Whether AI systems will be capable of actual thought is arguable—in part because of the intangibles that exist beyond the world of measured information but other factors as well. Independent of any technology or combination of technologies, this does not obviate concerns about the misuses of technologies. AI as it is defined today can also be viewed as transient in that there are things it cannot do and as such it is not an endpoint. So, we should be appropriately measured in our approaches, but vigilant as well, including dynamic approaches to mitigate and manage risks as they develop.

Global Perspectives

The factors driving a linear or non-linear world are global. The global nature of innovation presents novel challenges in how to develop guardrails while supporting economic incentivization. In a multilateral world, traditional approaches to strategic stability by maintaining technological advantage may not be successfully extended to encompass technologies of mass empowerment.

The speed and magnitude of new risk spaces will stress human social and political systems that typically lag behind in their development of strategies to counter them. Considerable vulnerability exists during this lag period. Considerations here include four dynamics suggesting the emerging domain is qualitatively different from the past, suggesting a phase change of global threat regimes.

1. **From point impact to distributed impact.** Technologies today enable bad actors to have disproportionate impacts such as the ability to intentionally create a systemic, networked impact. For example, AI or cyber-attacks may target energy distribution or banking systems that can have impact across an entire nation or coalition of nations. There is a qualitative difference between the geographic point being the target, and the economic or public health systems, or the undermining of democratic institutions, being the target.

2. **From blunt impact to precision impact.** New technologies can focus with surgical precision on very specific targets. From deepfakes to specific genotypes, or autonomous attacks, the nature of these technologies allow one to target entities across many scales.

3. **From nation states to individual actors.** Historically, high-impact attacks required the resources and commitment of nation states. With democratized technology, far-reaching attacks are becoming available to every level of threat actor, from individuals and small groups, criminal organizations, terrorist groups, and nations. With the explosion of emerging technologies, the character of these can be quite disparate.

4. **Enhanced covert action.** The use of democratized technology will increase the difficulty in identifying covert action and attributing it. For example, influence operations using social media to

[10] M. Heidegger, "What is Called Thinking," Max Niemeyer Verlag, Tubingen, (1954).

undermine trust in national norms and institutions is difficult to identify. Mobilization of defensive responses is likely to be chaotic and slow. Similarly, designer pathogens may prevent differential diagnosis from those natural occurring, obscuring them as a weapon.

The relative prioritizations of the sources of non-linearities will be unevenly reflected amongst our allies, partners, and competitors, from Arctic nations to those driving start-up-based innovation. Novel approaches to partnerships may be needed. Our combined endeavors may lead to different strategies and different risk frameworks and could inform different timelines for preparedness and response—this is how global actors operate. The democratization of advanced technologies raises deep questions on how to establish ethical standards, develop regulatory structures that do not stifle innovation, and maintain the norms of democratic societies. Broader and deeper international engagements is an important dimension to pursue in an ongoing manner. But in this age of innovation, historic approaches to new classes of problems will not be enough. We cannot afford different rules of the road for policymaking and developing next generation market products.

The Road Ahead

History is replete with examples of technologies that transformed the world, positively and negatively. Today, we have an opportunity to shape the future. With changes to law, economics, education, employment, and public safety, there are no single-point solutions on how best to prepare for and operate in the future world. Our ability to harness technology and bound it by our values, against the backdrop of a changing world, can only be accomplished by working with a wider cross section of society. The road ahead will be difficult, but it is not impassable.

Science and technology can open new avenues to manage risk, to attack problems, to support the manpower, means and technology approaches we use today so we are not always relying on surging as the only in-the-moment option for surprises. We need a suite of options we can turn to, that is complemented by a preparedness posture that allows less surprise and longer lead times to anticipate. This can be done in part by more awareness that we are entering into a non-linear world.

To compete and gain advantage in today's marketplace of ideas, it is important to recognize different regions and cultures of the world hold different perspectives and priorities. This is as true in North America as it is in Europe, Asia and beyond. New levels of scientific and technology cooperation are needed to ensure future technology advances are not unevenly reflected among our allies and partners. This same cooperation is needed to inform policymaking and shape new practices in emerging technology research, development, testing and evaluation. Recognizing the global implications to healthcare, commerce, defense, and security—no one organization or country, can do this alone. It requires collaborations across many levels, including academia, non-governmental organizations, private sector, government, and civil society.

This paper is not an exhaustive exploration of the changes that could be coming, but rather an invitation to imagine, and make real, a future world that is prepared for linear and non-linear events.

About This Paper

This paper is the first in a series of in-depth analysis on preparedness. S&T is examining how core investments in science and technology are yielding new options to ready the Department and nation for future change. This paper discusses the changing threat landscape and the unprecedented unpredictability of what's next in technological advances and the complexity of our current and future world and its likely non-linear nature. S&T—serving the greater homeland security enterprise with basic and applied research, development, testing and evaluation activities—is endlessly looking at current and over the horizon threats and growing an understanding of effective approaches to solve challenges in a world that is drastically shifting and requires many sectors, innovators, and partners to address.

Dr. Dimitri Kusnezov
Under Secretary for Science and Technology
U.S. Department of Homeland Security
July 2023