Risk Report

THE STRATEGIC SECURITY RISK REPORT

2019

Risk Group

Contents

The Strategic Security Risk Report 2019

The Strategic Security Risk Report 2019, 1st Edition, is published by the Risk Group. The information in this risk report, or on which this report is based, has been obtained from publicly available sources, Risk Group research, Risk Roundup discussions, and Risk Group analysis.

The Risk Group research, review, rating and reporting of the strategic security risks information makes no representation or warranty, express or implied, as many variables play a role in the onset of strategic security risks. The statements in this strategic security risk report may provide forecasting of future security events based on certain assumptions that are being made today by Risk Group. These forecasting statements are based on Risk Group analysis and involve many known and unknown security risks, uncertainties, and other factors emerging from across nations: its government, industries, organizations, and academia (NGIOA) in cyberspace, aquaspace, geospace and space (CAGS).

While the effort is made to research, review, rate and report all security risks arising from across nations for its strategic security impact, the risk research initiative is a work in progress, and future revisions will likely be made on a yearly basis as Risk Group research reviews more risks in a continually changing CAGS environment.

As a result, Risk Group readers are cautioned not to place undue reliance on these strategic security forecasting statements. Risk Group will not be liable for any loss or damage arising in connection with the use of the strategic security risk review information in this report.

Mission

Risk management, security, and peace are fundamentally integrated.

Although security is related to the management of threats and order is the outcome of successful conflict management, risk management is associated with the management of security vulnerabilities as well as the management of conflict, and it is not possible to conceive any one of the three without the existence of the other two. All three concepts feed into each other.

Risk Group believes that the security we build for ourselves is precarious and uncertain until it is secured for everyone.

About Risk Group

Risk Group LLC (https://www.riskgroupllc.com) is a leading strategic security risk research and reporting organization. It is a private organization committed to improving the state of global resilience through collective participation and reporting of critical, interconnected risks across cyber, aqua, geo, and space (CAGS). In the spirit of global peace through risk management, Risk Group engages with individuals and entities across nations: its government, industries, organizations, and academia (NGIOA) to provide a system's level view of independent and inter-dependent, integrated risk and shape the dialogue on collective risk management. Incorporated as a limited liability corporation and headquartered in Sugar Land, TX, Risk Group is an independent organization that prides itself on not being tied to any special interests.

Our history, from hunter-gatherers to the first agrarian societies to the rise of vibrant and innovative civilizations around the world, demonstrates not only an ability but a skill at working together towards a better future. We carry the genes of the forward-thinking members of our species: the ones who wisely chose to pool resources, work together, and overcome hardship, rather than suffer in isolation and perish. These visionaries are our ancestors; we wouldn't exist were it not for the wisdom of their choices.

Today, as we contend with a myriad of economic, political, technological, sociological, and planetary risks, Risk Group strongly believes that we must revisit our origins and collaborate at the individual and institutional levels. Similar to the existential threats our ancestors overcame thousands of years ago, our species is now at a crossroads where we can collectively ascend to the next chapter or lose everything that our forefathers fought so hard to build. We evaluate critical risks from a systemic standpoint, rather than focusing on discrete silos, with a persistent focus on improving the capacity of global risk management infrastructure across governments, industries, organizations, and academia (NGIOA).

Introduction

Science and technology are advancing rapidly. Recent progress in quantum physics, biotechnology, nanotechnology, genetics, artificial intelligence, robotics, drones, 3D printing and more is proving to be disruptive. These technologies, individually and collectively, have the potential to benefit humanity significantly. However, these same disruptive technologies can enable the development of asymmetric, next-generation weapons against which we are not yet prepared.

In this era, the pace of technological development has surpassed a nation's ability to govern effectively. The gaps and vulnerabilities between emerging technologies and governance models are visible across cyberspace, aquaspace, geospace, and space (CAGS). We live in a time where security risks emerging from the threat of autonomous-weapons, bio-weapons, nano-weapons, cyber-weapons, and more are so dire that there is no alternative but to start thinking about how the future of humanity will be affected. While there are some siloed efforts focused on managing the risks of artificial intelligence, the lack of focus on existing and emerging dual-use technologies across the contested commons of CAGS and their emerging security risks is becoming a cause of great concern.

These dual-use technologies are re-writing the rules of information, intelligence, survival, and security. It is said that the better the strategic security intelligence, the better the strategy for human survival and security in CAGS and beyond. Since strategic security intelligence furthers our advances towards individual and collective goals for humanity beyond CAGS (by suggesting ways to adapt and/or manage around an array of CAGS risk variables and opportunities), understanding strategic security risk intelligence is fundamental for individuals and entities across nations: its government, industries, organizations, and academia (NGIOA).

It is one thing to gather strategic security risk data and extract information, but it is an entirely different thing to turn that information into meaningful and actionable strategic security risk intelligence. Strategic Security Intelligence must provide information that can be acted upon by everyone, individuals, and entities across NGIOA if it is going to be deemed of value for the security of CAGS.

A challenge of our time is that the market for intelligence is now politicized and largely about providing information that makes decision makers feel better. The survival of humanity necessitates developing insights about integrated CAGS security risks. It matters that we all understand strategic security risks and that we all have access to much-needed intelligence to play a role in shaping the future of humanity.

Security is no longer a government affair. It's an NGIOA affair. Security is no longer about geospace security. It's about CAGS security. It is this new emerging security paradigm that we at Risk Group are focused on. We hope you join our efforts for the future of humanity.

Jayshree Pandya, Founder and CEO, Risk Group LLC

The Top 10 Strategic Security Risks Facing Humanity

1	Dual-Use Technologies
2	Clash in Contested Commons
3	Failing Governance Models
4	Quantum Physics and Technologies
5	Technological Singularity
6	Integrity of Information: Disinformation and Misinformation
7	Growing Natural Disasters
8	Social Isolation and Loneliness
9	Natural Resources: Scarcity and Geopolitics
10	Antibiotic Resistance

Dual-Use Technologies

Irrespective of nuclear, quantum, biological, genomic, chemical, electronic, digital, or nanotechnology, the pace of science and technology developments are exponentially increasing the dissemination of dual-use products across the CAGS ecosystem.

Biology and Bio-Weapons

Biological/Germ warfare is a growing threat to the future of humanity. Any use of bacteria, virus, fungi, or toxins to destroy a target, military or civilian, continues to be a cause of great concern. While the use of biological weapons is considered a war crime by the UN Biological Weapons Convention, the reality remains that emerging biological weapons will be difficult to detect and stop on time. As a result, the number of biological organisms that could harm is increasing exponentially. Biological/Germ warfare is rapidly becoming a growing threat to the future of humanity.

Genetic Engineering and Gene Editing

In the coming years, we will be able to design and build any cell, organism, or biological species we want, with a growing selection of genomic data from human, non-human and or any other living species. We are close to the point where our ability to create or manipulate "life" will only be restricted by our imagination. In the not-too-distant future, we will be able to build any cell, organism, or biological species up from scratch.

Information Technology and Computing

The evolution of computer technologies and computing has democratized computing power. Questions are being raised about how to manage the potential threat posed by information technology, whose growth and proliferation position information warfare in the elite club of technologies capable of unleashing massive harm. The application of information and communications technology as a weapon is a growing cause of security concern.

Cyberspace and Cyber Weapons

Code and servers have connected cyberspace to aquaspace, geospace, and space. As a result, everything is controlled or goes through cyberspace. At the same time, weapons are also being developed that are computer-controlled. As we see: encryption has dual use, cyber-attacks have a dual purpose, cyber threats have a dual purpose, and information has a double meaning. Intelligence has a dual purpose.

Since cyber weapons can be used for beneficial purposes and misused for harmful purposes, they constitute a dual-use technology of concern.

Cyberspace has made it easier for anyone to spy on anyone. Cyber weapons are routinely used to steal money, commit fraud, seize trade secrets, destroy data, render information systems inoperable, and damage machinery controlled by computers.

Artificial Intelligence and Autonomous Weapons

There is growing concern about emerging autonomous machines. Autonomous weapons can be efficiently coded to identify a target and decide to open fire without needing to check with a human decision-maker first. As the notion of an autonomous weapons system moves from concept to reality, it is becoming a cause of great concern as to how humans will regulate such capabilities.

Electromagnetic Spectrum and EMP Weapons

Affordable, accessible dual-use technologies are the pre-eminent strategic security risk facing humanity as they fundamentally take power (both good and bad) from a select few and give it to the masses.

When each nation today increasingly depends on tightly integrated, high-speed electronic systems, a tiny weapon can also give a country's enemies the ability to use the electromagnetic spectrum (signals like radio, infrared, or radar) to deny those nations the ability to use these radio signals for their digital systems, connectivity, and infrastructure.

As a result, emerging EMP weapons change the nature of warfare and shake the very foundation of security and peace.

Nanotechnology and Nano-Weapons

In the coming years, nanotechnology will bring to reality nano-robots and micro-robots for nano-scale devices and systems. These can enable various helpful medical applications, such as targeted medicine, cancer research, and early detection systems. However, it may also bring to reality unique biological weapons, nano-bombs, nano-engineered self-multiplying deadly viruses, and more.

Dual-use technologies have the potential to change the world for worse. It is vital to evaluate all emerging dual-use technologies and create risk mitigation strategies to defend not only ourselves but the very future of humanity in this growing spectrum of CAGS conflict.

Clash in Contested Commons

As the contested commons of cyberspace, aquaspace, geospace, and space (CAGS) offer each nation as many opportunities as they do challenges, the upcoming clash brings critical security risks for the future of humanity.

The contested commons are growing in number, nature, and nuances. In addition to geospace, space, cyberspace, and aquaspace are now also contested commons. While no nation owns or controls any of these contested commons, over the years, the order within these spaces was effectively managed through the existing power dynamics between nations. Nonetheless, the emergence of cyberspace has fundamentally disrupted all other contested commons and the very global order.

Cyberspace brings nations substantial strategic value in all the contested commons. With the right technologies and strategy, any country today can benefit from cyberspace. And, due to cyberspace, this is also true of geospace, space, and aquaspace. Everyone has a right to cyberspace. While everyone should have access to cyberspace, the on-going integration of cyberspace (and its speed and scope) with other contested commons brings both security perils and promise.

Governing the commons of cyberspace is proving to be complex. This is also true of ensuring security. The whole world is on their own and must provide for their protection. Nations do not have an effective way to control what happens outside their borders in all contested commons, nor can they fully control what happens within their borders. These evolving security dynamics are reshaping global power dynamics, as well as how power is shared within and across national boundaries. Therefore, the world is undergoing an inevitable and perhaps irreversible change in the relative balance of power dynamics across CAGS.

In the coming years, each of the contested commons is expected to face extraordinary changes and challenges. Individually and collectively, the approaching clash of the contested commons is on its way to disturb the pre-existing global order and, therefore, is a critical risk facing humanity.

Failing Governance Models

Existing governance models are failing in the face of emerging technologies, systems, and technological transformations. The fear of any ground-breaking technology or technological transformation, and its associated changes and challenges calls for governments to regulate these new technologies responsibly.

While this is nothing new, regulating emerging technologies like artificial intelligence, quantum technologies, gene editing, and more is an entirely different kind of challenge.

Each of these emerging technologies can be misused. They can also behave in unpredictable and harmful ways towards humanity and could put human civilization at risk. In the much-needed discussions on governance, we see positive efforts to discuss ethics and privacy – however, a rigorous dialogue on security implications remains notably absent.

Overall, we are not governing and regulating emerging technologies, proactively, and responsibly. The lack of effective technology governance models is a critical risk facing humanity.

Quantum Physics and Technologies

The concept of entanglement is at the core of much of applied quantum physics. The commonly understood definition of entanglement says that particles can be generated to have a distinct reliance on each other, despite any three-dimensional or four-dimensional distance between the particles.

What this definition and understanding imply is that even if two or more particles are physically detached with no traditional or measurable linkages, what happens to one still has a quantifiable effect on the other. Now, individuals and entities across NGIOA are part of an entangled global system. Since the ability to generate and manipulate pairs of entangled particles is at the foundation of many quantum technologies, it is vital to understand and evaluate how the principles of quantum physics translate to the survival and security of humanity.

Advances in quantum physics and technologies bring a transformative potential to advance many complex industry solutions. From the energy industry to finance, healthcare, and aerospace, many industries will likely benefit from the transformative potential of quantum physics. However, quantum communications, quantum computing, and potentially quantum radar will change the security and defense landscape. In the face of this technology, modern information-centric defense apparatuses – with sophisticated intelligence systems, satellites, secure communications networks, and stealth technologies – will face complex security challenges.

Each of the advances in quantum physics and technology is expected to bring extraordinary changes and challenges in the coming years and will put enormous pressures on these contested commons. Individually and collectively, the transformative potential of quantum physics and technologies will likely trigger the disturbance of global power dynamics. This is a critical security risk for the future of humanity.

Technological Singularity

A technological singularity reflects the commonly believed idea that an intelligence explosion and its associated changes may happen suddenly. As a result, it will be difficult to predict how the resulting new world would operate.

We stand today on the periphery of a technology-triggered revolution and evolution in not only information and intelligence but also gene editing and genomics. These advances in technology finally give humans an ability to change an organism's DNA with precision. Today, technologies like CRISPR allow genetic material to be inserted, deleted, modified, or replaced. Gene editing tools bring great potential for humanity to move beyond natural evolution, and humans gaining the control to evolve on their own terms and timeline seems inevitable. The scale, scope, and severity of the impact of the artificial intelligence and gene editing revolution is unlike anything our species has faced before.

The rate at which the revolutionary innovations are emerging in artificial intelligence, and gene editing has no historical precedent. It is fundamentally disrupting everything in the human ecosystem and even moves the very evolutionary process towards human control. The breadth, depth, and impact of the intelligence evolution herald the essential transformation of entire interconnected and interdependent systems.

Irrespective of whether the technological singularity will happen through artificial super intelligence or gene editing, the very concept raises many fears and critical security risks. There is no way to forecast just how and when either or both of these technologies will evolve. Given the lack of direct evolutionary motivation for a new intelligent species, it is further unclear whether a human-made intelligence explosion of this kind would be beneficial or harmful, or even an existential threat, to the future of humanity.

It is challenging to have an exact timeline or consensus on when superintelligence in man or machines is likely to be achieved. But it is time to begin a discussion on what we want as a species for ourselves and our ecosystem. Both AI and gene editing have the power to change the very fundamentals of human evolution, survival, and security, and the response to it must be integrated and comprehensive.

The Integrity of Information: Misinformation to Disinformation

Information is a critical dimension in today's warfare. Most individuals today do not have the expertise, skill set, and resources to evaluate the integrity of information – and as a result, are vulnerable to today's misinformation and disinformation campaigns. Since knowledge is the source of power, not having credible information weakens the strength of informed decision-making. It is therefore essential to acquire new skills and competencies to differentiate credible information from the onslaught of misinformation and disinformation.

When information is created, produced, or distributed to harm a person, social group, organization, or a nation, and there are no effective laws to protect the vulnerable, society succumbs to a false reality. As seen in the world today, this contributes to dramatic polarization and leads to severe damage to society's social fabric.

Left unchecked, a lack of information integrity and the erosion of facts ultimately contributes to society's collapse. A lack of information integrity is a critical security risk facing humanity. We must develop useful tools and techniques to avert this decline.

Natural Disasters

From hurricanes to wildfires, to cyclones, natural disasters are growing in number, size, strength, and impact. While we've always faced natural disasters, we are currently observing a scale of disaster and destruction that is deeply concerning.

Emerging disasters are increasing in size and strength. The UN Intergovernmental Panel on Climate Change (IPCC), as well as researchers and scientists worldwide, have warned of an impending climate catastrophe related to global heating and human pollution and activity, which contributes to these harsher disasters.

We lack all the answers we need as the science of the earth and its environment is complex, under-evaluated, and still being understood. Amidst the complex challenges of our planet's environment, managing these risks is an even tougher challenge, as fear, ignorance, denial, and misplaced priorities compound them.

Since the earth's environment is an essential component for human existence, it is fundamental to ensure its sustainability. We must confront natural and human-made changes to our environment. There is a need for collective effort, initiatives, and investment in ensuring we use the aggregate intelligence of our species and the technologies we've developed to protect our planet. It is time to apply collective intelligence to save the human ecosystem.

Loneliness

Loneliness – or a state of chronic perceived social isolation -- in all age groups is a growing global problem.

As the late Dr. John Cacioppo's research underscored, loneliness increases the risk of developing a range of disorders, from cardiovascular disease, neurodegenerative diseases, cognitive decline, and metastatic cancer. It weakens the human immune system, and if left unchecked, can affect brain structures and human decision-making processes for the worst.

Considering our origins as a tribal species, we did not get here overnight. A range of factors has contributed to loneliness today. Professional lives are increasingly transient and uprooting your life for a job opportunity is the expectation. The rise of remote working, while offering flexibility, meaningfully reduces social interactions. Outside of work, meeting new people can be a struggle, as we have a few shared community institutions. Stress levels show no sign of abating, and technology has reduced our need for in-person interactions[1]. People of all age groups, including our senior citizens, increasingly live and age alone.

The loneliness epidemic is expected to increase in size and complexity. Therefore, the declining emotional well-being of humans is a critical security risk facing humanity. Meaningful connections and relationships are fundamentally biological needs and vital for mental and physical health. Serious efforts need to be made to combat widespread loneliness – in the absence of remedies, declining life expectancy, and productivity will be the new norm.

[1] This is, understandably, a nuanced topic. For example, technology has done wonders for *maintaining* human connection; diasporic and immigrant populations can maintain relationships with friends and relatives much more effectively thanks to video conferencing and social media.

Natural Resources: Scarcity and Geopolitics

As we witness unprecedented growth in the human population, the question arises: do we have sufficient natural resources to sustain the human race? Natural resources such as clean air, water, and soil or carbon, nitrogen, and nutrient cycles are basic life support systems of the earth.

On the Horizon: Space Mining

Natural resources are essential for not only human survival but also technological progress and development.

As nations begin to make serious efforts towards space mining, the very fact that quadrillions of dollars of valuable material is hiding in near-earth asteroids will undoubtedly lead to the weaponization of outer space. This is an impending security risk facing humanity.

While space mining, exploration and interplanetary travel are becoming essential for the future of humanity, it is important that nations agree on a space resource framework that enables transparency, fairness, and collaboration -- one that unites us in a better future for all of humanity, not just a select few.

The intense pressures of population growth (often resulting from rapid economic growth) are placing incredible pressure on finite, non-renewable natural resources such as fossil fuels and minerals. In the coming years, it is expected that the demand for these resources will only increase.

Natural resources are essential for not only human survival but also technological progress and development. As a result, finding, creating, and producing more resources has become a survival necessity for humans. Emerging technologies and initiatives like synthetic biology, molecular manufacturing, asteroid mining, and more will give humans the much-needed ability to find solutions to the problem of natural resource scarcity. Until we discover solutions, however, there will be global competition for the remaining deposits of minerals and fossil fuels (especially shale gas).

In response to this dynamic, many nations' governments are ramping up their resource protectionism efforts. This is just the beginning of many geopolitical events that will create complex security risks for the future of humanity. This competition will undoubtedly play into the security risks arising from natural disasters and climate change. Our best hope for avoiding this fraught geopolitical landscape is technology.

Antibiotic Resistance

The rapid emergence of resistant bacteria is occurring across nations. As a result, any simple bacterial infection is becoming a threat to human life. Pathogens affecting humans and other species alike are increasingly becoming resistant to antibiotics or chemicals. As a result, the growing number of communicable and non-communicable human and non-human infections is becoming extremely difficult to treat.

Antibiotic resistance is a growing crisis with huge strategic security implications. It is not only humans that are at risk of the ever-increasing antibiotic resistance but also animals and other living species. We only need to look to the 1918 Spanish Flu pandemic, which killed 3 to 5 percent of the world population, or the 2014 Ebola outbreak to understand the danger of this risk.

The scope of the problem is enormous. This is especially true given how quickly infections can spread due to urbanization and global transportation networks. Nations can promptly overcome by the sheer numbers and logistics of an outbreak, and many have urged nations to craft policy with foresight. Unfortunately, nations often boost up disease control measures only during a crisis and re-appropriate those funds elsewhere after the crisis subsides.

Antibiotics no longer being the first line of defense has enormous implications for human health. As the human race enters the post-antibiotic era, the question we need to evaluate is whether we have alternate tools to save humanity from the next generation of infections coming our way.

Nature of Security Risks

While we have briefly discussed the top ten strategic security risks facing humanity, many other strategic security risks also need serious attention. From disappearing jobs and loss of wages to mass migration and social unrest, there are many emerging security risks that we all collectively need to pay attention to. Risk Group will make all efforts to discuss each of these risks in the coming months and years.

To manage any strategic security risk, an effective global governance system needs to be defined and designed—that is enforceable, transparent, accountable, valid, legally binding, collaborative, and can be trusted by everyone.

It is a cause of great concern that the materials and methods for creating weapons of mass destruction are readily available and that the cost of materials to construct or produce a weapon is low. The current governance models are proving ineffective. Given the implications for making bioweapons, nano-weapons, cyber-weapons, or e-weapons, we need to understand the dangers that advances in science and its democratization may bring to us.

Moreover, the growing "do-it-yourself (DIY)" movement is providing the necessary information, infrastructure, and open access of ideas and intelligence to enable anyone and everyone from across nations an ability to access all the required resources to build, synthesize, grow, and create whatever they desire. This has given an individual the ability to explore, to experiment, or to test any hypothesis. While we often celebrate this democratization, we must also be aware of the dangers this can create.

The multifaceted security challenges necessitate an evaluation of how any individual or entity from across nations can explore fundamental science without any accountability, oversight, and consequences. The reality today is that any new idea, innovation, and invention might be used for both beneficial and harmful purposes. Therefore, we all need to recognize that, while such ideas, innovations, and inventions are driving the innovation landscape of nations that provide essential applications for their vital needs and economy, they can also very well lead to the production of unprecedented weapons of mass destruction. This could potentially bring existential risks to the future of humanity.

Building Resilience

Security risks are growing in all contested commons. So, if we are to protect our hard-fought progress and development in cyberspace, aquaspace, geospace, and space (CAGS) by managing security risks developing from emerging technologies, technological transformation, and natural and human-made disasters, building resilience must be a priority for everyone.

Nations will thrive when resilience is an integrated component of its ecosystem. The ability of any nation and all its components to anticipate, absorb, adapt to, and prepare for any potentially disruptive event in cyberspace, aquaspace, geospace, and space depends on its understanding of risks and resilience. Since disasters, risk, resilience, and security walk hand in hand, it is essential to understand how to manage security risks from cyberspace, aquaspace, geospace, and space.

Any attempt to reduce the strategic security risks in CAGS is an effort towards building a resilient human ecosystem. Decision-making impacts the level of resilience in CAGS. The perceptions of and choices made about security risks will likely shape how individuals and entities across NGIOA will behave, how they will respond during and after a security event irrespective of CAGS, and how they will plan for its future security.

Resilience, the ability to overcome challenges from cyberspace, aquaspace, geospace, and space, is fundamental to developing security protection mechanisms for nations. Understanding security risks and resilience methods across CAGS is therefore crucial to the future of humanity.

Risk Group Call for Action

With this Risk Report, Risk Group is hereby calling individuals and entities across NGIOA to come together and collaborate to help research, review, rate and report the risks emerging from across nations in CAGS. To join Risk Group efforts, please email Risk Group at info@riskgroupllc.com.

About Risk Group's Founder And CEO

Dr. Jayshree Pandya (née Bhatt), Founder and CEO of Risk Group LLC, is an expert in disruptive technologies. She is a globally-recognized thought leader driving discussions on resilience, risk management, and national preparedness.

Jayshree's doctorate work in the 1980s focused on hydrogen production by Halobacterium halobium, for which she received India's National Young Scientist Award in Biochemistry.

Her publications on this work have been cited in several books, journals, and reports published by governments, including a report from the United States Department of Energy. Her work on anti-cancer drugs also received worldwide attention and, amongst other citations, has been referenced in a report published by the World Health Organization. In 1991, she was invited to come to the United States (under the Scientist Exchange Program) to continue research on hydrogen production and was awarded a post-doctoral fellowship at the Hawaii Natural Energy Institute. After that, she researched atherosclerosis at the University of Chicago Medical School. Next, she took a job at Aurotech, a biotech company based in Wisconsin. As in her Ph.D. research, she used microorganisms to develop natural processes and technologies.

While her doctorate and post-doctorate studies gave her the first taste of the power of interdisciplinary research, it also introduced her to the repressive power of institutional silos and inefficiencies. As a result, her physical location wasn't the only thing that shifted in the 1990s; her focus did as well.

Since Microbiology trained her to see changes in tiny organisms coming from natural selection, she began to see similar forces at work in the evolution of individuals as well as entities across NGIOA and society in general.

It's all the same underlying mechanism. Her career took another turn after she was asked to consider risk management as part of a strategic planning effort by one of her employers. She quickly realized that most risk management is all process, with no real benefit. That was the beginning of Risk Group, the strategic security risk research organization she founded in 2002, from where she is passionately creating and managing cutting-edge security ventures that bring a futurist perspective to nations and all its components to improve innovation capacity and to define and design new ideas, innovations, products, and services for security and sustainability.

From the National Science Foundation to organizations from across nations, Jayshree is an invited speaker on emerging technologies, technology transformation, digital disruption, strategic security risks, industry risks, and country risks. She is the author of the book, The Global Age: NGIOA @ Risk and has also published many scientific and technical papers. Jayshree advises decision-makers at all levels on existing and emerging technologies: emerging applications, impact, and solutions.