Risk Report 2020

The Strategic Security Risk Report 2020

Second Edition

Risk Group

Content

The Strategic Security Risk Report 2020

The Strategic Security Risk Report 2020, 2nd Edition, is published by 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 Group's 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: their government, industries, organizations, and academia (NGIOA) in cyberspace, aquaspace, geospace and space (CAGS).

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

About Risk Group

Risk Group LLC (https://www.riskgroupllc.com) is a leading strategic security risk research and reporting organization, a community, ecosystem, and a collective strategic security risk analytics platform. Risk Group's strategic security community and ecosystem is the first and only collective community that is made of cross-disciplinary and top scientists, security professionals, thought leaders, entrepreneurs, philanthropists, policymakers, educators, corporations and organizations from across nations collaborating to research, review, rate and report strategic security risks to protect the future of humanity.

Risk Group actively collaborates with decision-makers from across nations to identify what ideas and innovations are essential for the survival and security of nations and the human species. The strategic security community, ecosystem, and platform support collective ideas, imaginations, and innovations, from basic science research to commercial ventures to bridge the security gaps across cyberspace, aquaspace, geospace, and space. As cyberspace blurs the boundaries of aquaspace, geospace and space as well as individuals and entities across nations, the growing vulnerability necessitates mapping of the security risks. Our focus is to collectively map the security risks, define a security-centric operating system for humanity, build a strategic security roadmap for effective forward progress in the science of security with NGIOA decision-makers, and focus particular attention on the ideas and innovations that are essential to bringing security to the human CAGS ecosystem.

Risk Group 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 interdependent, integrated security risks and shape the dialogue on collective security risk management and governance. 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 would not 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. Like 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.

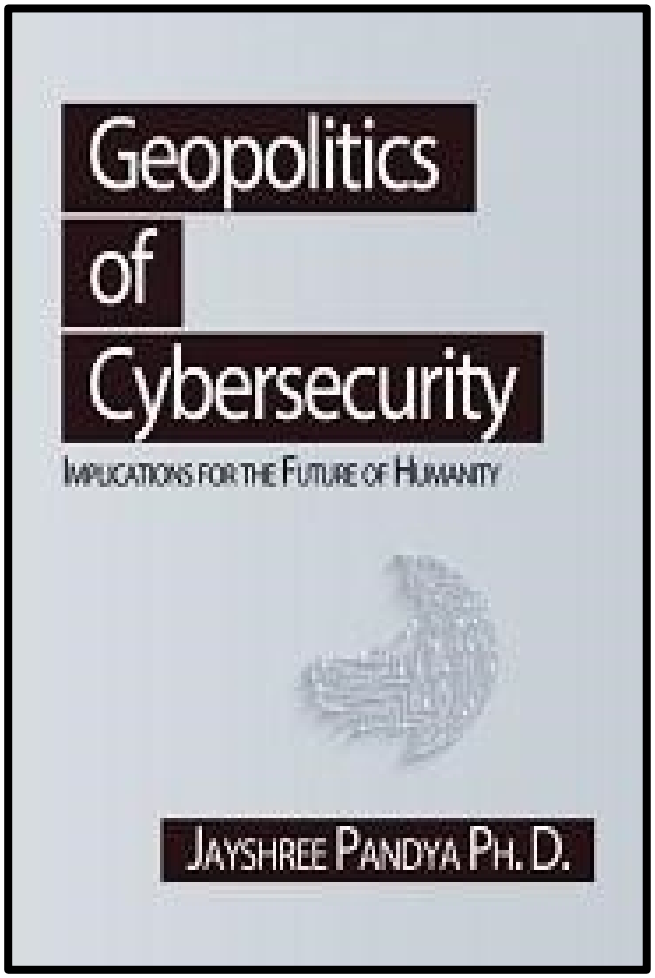
Introduction

The second edition of Risk Group's Strategic Security Risk Report 2020 is published as digital disorder is rising and the geopolitics of cybersecurity is threatening the contested commons of cyberspace, aquaspace, geospace, and space. In addition to economic and security implications, the threat to the future of humanity necessitates we define a path for collective action for our collective security. The reason is cyberspace is human-made and is connecting everyone, humans as well as machines. The rapidly evolving interconnected human NGIOA/CAGS ecosystem is on its way to bring a fundamental transformation to the way we live, work, do things and more. While the interconnected CAGS ecosystem has allowed nations to redefine and redesign the systems at all levels, the rushed transition to the emerging connected systems (which went forward without us first understanding the associated risks and having in place proper change management processes) is failing to promote progress and advancement for everyone. As a result, amidst the echoes of failed globalization and the rise of digital disorder, the growing concerns of the emerging turbulence are giving rise to social, political, and economic chaos.

The powerful forces of democratization of constructive and destructive ideas, imaginations, and innovations are proving to be disruptive at all levels across the entire CAGS ecosystem. Every individual and entity across NGIOA, every component of a nation is impacted. Despite that, nations are struggling to keep up. Amidst the democratization of destruction, do-it-yourself movement, shifting surveillance power, commoditization of intelligence, and the lack of integrated NGIOA approach, decision-makers today are ill-positioned to address the vulnerabilities of emerging technologies, technology transformation and its associated changes. This is visibly seen in the design, development and deployment of cyberspace technologies like AI, 5G and more.

AI-driven surveillance technology is not only bringing fundamental transformation to surveillance and sabotage but is also shifting the power structure and the nature of power. The technology layers from cyberspace are creating new power centers. The new mode and nature of intelligence are disrupting traditional alliances.

Understandably, the geopolitical risks and the environment are driving the Strategic Security Risks for 2020.



It is fitting that this year's Risk Report coincides with the Risk Group publication of the book, Geopolitics of Cybersecurity: Implications for the Future of Humanity. The book focuses on the rapidly emerging technological transformation from cyberspace that is fundamentally altering aquaspace, geospace, and space (CAGS). Amidst a backdrop of increasing global competition, mistrust, disorder, and conflict, there are many growing concerns for the future of humanity. Conversations about cyberspace and technology are now inextricably linked to broader conversations affecting each one of us across nations, from trade policy and digital autonomy to cyber warfare and the weaponization of artificial intelligence. As a result, the geopolitical forces are shaping not only the future of nations but also the future of humanity. Ultimately, how nations handle these issues and conflicts will determine the future of humanity.

Jayshree Pandya, Founder and CEO, Risk Group LLC

The Top 10 Strategic Security Risks Facing Humanity In 2020

1	Geopolitics of Emerging Technology
2	Algorithmic Warfare to Asymmetric Hybrid Warfare
3	Declining Trust in Technology and Rising Digital Disorder
4	Failing Governance Models and Growing Protectionism
5	Natural and Human Made Environmental Disasters
6	The Integrity of Information and Mass Manipulation of Human Minds
7	Social Isolation, Loneliness, and Mental Health
8	Rise of Infectious Diseases, Pandemics and Nation Preparedness
9	Declining Civilization thinking and Rise of Tribalism
10	Collapsing Systems and Economic Uncertainty

1. Geopolitics Of Emerging Technology

The world is seeing the beginning of the fundamental transformation of its CAGS ecosystem as disruptive innovations began to emerge at a breakneck speed.

The making of cyberspace and the advances in emerging technologies shaped the digital age. Information and communication technologies became a core driver to globalization that gave nations faster, cheaper and more efficient flow of freights and services. With the rapid advances in broadband and satellite communications and the rapidly accelerating microprocessor speed, and abundant energy, the global systems were on the rise.

Nations began to come together. Globalization emerged where manufacturing and research and development began to be outsourced to developing countries. However, that did not last long, as the making of cyberspace became much more complex and digital order began to turn into digital disorder due to the geopolitics of cybersecurity. The reason is, in addition to the information and communication technologies, many other layers of technology began to be added to cyberspace. From artificial intelligence to blockchain, internet of things to 5G, and cloud computing to quantum computing, the revolution brought on by cyberspace technologies in addition to the advances in basic sciences of biotechnology, nanotechnology, and more rapidly emerged. Understandably, the battle for each layer of cyberspace technology is intensifying. Irrespective of whether it is an AI layer, blockchain layer, IoT layer, or 5G layer, nations are competing to establish their digital supremacy in the rapidly evolving connected human CAGS ecosystem. In the end, it will perhaps be the computing power, ideas, and imagination that will determine which nations will be able to compete and plant their flag of supremacy in cyberspace as they march forward.

5G, the fifth-generation telecommunication power, is rapidly becoming an aggressively contested technology since it, in addition to computing power, can drive the rapid movement of growing data that will also play a central role in the on-going industrial revolution. As 5G opens up the closed internet of thing ecosystem, the enormous growth in data will further drive intelligence power. Advances in AI, especially machine learning, are driving the rapid evolution of the intelligence spectrum. Sensor embedded

internet of things and AI are driving the automation across NGIOA further. 3D printing and digital additive manufacturing are redefining the very meaning of manufacturing and production. Smart Grids, Smart Energy, and advances in energy technologies are also driving the decentralization of energy. Many fundamental advances in how we compute are also emerging.

Each of these technology layers brings disruptive potential and is at the center of the global power play. The reason is that emerging technologies are closely tied to geopolitical affairs. While the geopolitical competition amongst nations is a significant driver to the on-going industrial revolution, it is also shifting the balance of power and is triggering critical security risks for the future of humanity. Geopolitics of emerging technology is at the top of the 2020 Strategic Security Risk Report.

The technology layers of cyberspace, the algorithm that will control the data and information flow, will give enormous intelligence power to the nation that controls the algorithm. Amidst the lack of security controls to the data and information flow, the wild west of cyberspace has triggered geopolitical warfare. At the heart of the geopolitical battle is which nation will innovate and control the global data flow, and thereby the global information and intelligence flow.

Moreover, when cyberspace has connected aquaspace, geospace, and space, the geopolitical battle of emerging technologies is trickling down to aquaspace, geospace and space. This has put the entire human CAGS ecosystem at risk and has become a top strategic security risk facing humanity in 2020.

The making of cyberspace has leveled the playing field and democratized the power of innovation. Since each nation's economic and national security are tied to the respective nations' innovation engine, where the next disruptive innovation comes from is and will be at the center of the global power play. The nations that will not be able to compete will likely collapse and turn to traditional means of warfare. As a result, the warfare spectrum has become enormous, putting a strain on security and military professionals. If cyberspace is not security-centric and our efforts are not towards defining security in our human ecosystem, while emerging technologies hold great promise, the geopolitics of cybersecurity will bring critical strategic security risks for the future of humanity for which no one is prepared or will be prepared in any meaningful way.

2. Algorithmic Warfare To Asymmetric Hybrid Warfare

The nature of warfare is changing and evolving in the human CAGS ecosystem. As we see advances in the making of cyberspace, drone technology, artificial intelligence, robotics, cyber warfare, the militarization of space, synthetic biology and more that can manufacture life or bioweapons, warfare seems to be undergoing a fundamental transformation. In the coming years, the future of warfare will likely be shaped by the role of miniaturization of drones, robots on the battlefield, cyber weapons, growing surveillance and sabotage capabilities, the militarization of space, the emerging potential for bio-weaponry, nano-weaponry, EM-weaponry and more.

Synthetic biology, the scientific manufacturing capability of life, the proliferation of autonomous drones and weapons, and the increasing opportunity of algorithmic warfare are just the tip of the iceberg in the emerging warfare spectrum. The evolution of surveillance technologies, EM weapons, space weapons, autonomous unmanned systems, artificial intelligence-based robotic weapons, technologies to manipulate masses, and more are transforming warfare fundamentals.

As seen, wars have already gotten smaller, are generally not declared, and are even won without the need to fire a single shot or missile. The fact that wars can happen simply when individuals, groups, or nation/states, armed with information and intelligence, create the conditions for hybrid warfare to achieve their strategic objectives is understandably alarming everyone. In a human ecosystem that is increasingly dependent on technology from cyberspace, as the nature of warfare evolves and becomes hi-tech, so does the dividing sovereignty lines blurring across NGIOA/CAGS.

There is no doubt that algorithmic warfare is emerging rapidly. Reports are emerging of the rise of autonomous robots and drones from China. While most nations have refrained from autonomous weapons, the reality remains that algorithms are on their way to changing warfare fundamentally. This vicious, algorithm-driven power struggle, raging on across CAGS, is full of unknowns, including major players, minor players, and rules of algorithmic/asymmetric warfare. In these connected CAGS battlefields, the

concern is no longer just on the war casualties quietly piling up due to cyber-attacks, but it is also on what autonomous algorithms will do next, irrespective of whether they are integrated with weapons or not. Questions are emerging of whether autonomous algorithms will self-evolve, and if they do, where would they go, and what would they do. It seems everyone will be vulnerable from the rising threats of autonomous robots and weapons. Any war that will be fought without the involvement of humans could prove disastrous for the future of humanity. We need to ask ourselves, have we visualized a war between algorithms? What could it look like? How would we stop it if it gets out of control?

Part of preparing for warfare is understanding it. The question is whether we effectively understand on-going asymmetric hybrid warfare across CAGS.

3. Declining Trust In Technology And Rising Digital Disorder

There is growing consumer and geopolitical distrust in cyberspace technology. There is a growing debate on whether the technology layers that make cyberspace can be trusted. As the trouble with the trust in technology increases, the question is whether geopolitical distrust is misplaced.

It seems the lack of trust in technology originates from the intentional and unintentional security vulnerabilities that get embedded in hardware, software, and other components that make cyberspace. The backlash to technology, the techlash from cyberspace, also has a lot to do with technology companies and their lack of accountability towards the security of their products and platforms. Politicians are already calling for the breakup of big technology companies. The question is whether that is a sensible solution over creating necessary systems of governance, regulations, and systems that allow enforcing accountability. Perhaps it is time to define and develop a consumer protection agency with embedded checks and balances to ensure trust in technology.

This is especially important when nations are actively driving information warfare to prove the supremacy of their culture, religion, way of life, and more. Furthermore, the destructive potential of emerging technologies is not only about the potential loss in jobs, but a loss in privacy and security as well. So, as trust in technology declines, it is essential to understand the role this plays in driving consumers away from cyberspace technology and the implications for the future of humanity.

While cyberspace technologies are a force for good, they are dual-use in nature. If the confidence in these technologies declines and the trust is shaken, it has enormous economic and security implications. Technological evolution cannot happen without trust and acceptance from its users, the consumers. According to the data from the Pew Research Center, Americans have become much less positive about technology companies' impact on the United States. This trend is perhaps seen across nations.

It is vital to begin a discussion on how to bring trust in technology back. It is time to discuss how to bring integrity to information, intelligence, news, and sources. It seems that unless we build effective systems, agencies, and institutions, technology from cyberspace will not flourish in the way that it was intended. The trend of digital order reversing and moving towards digital disorder will create enormous risks that will likely impact the future of humanity.

4. Failing Governance Models And Growing Protectionism

Existing governance models are failing in the face of emerging technologies from cyberspace, the connected CAGS systems, technological transformations, and rising digital disorder. The reality is that emerging technologies are advancing at a speed where the rules and standards for governance do not exist. Nations are overwhelmed in keeping up with the impact of emerging technologies and are aggressively trying to transform their businesses, systems, industries, and models to be able to benefit from the power of emerging technologies.

Moreover, the nature of emerging technologies is much different from previous technologies over the years. Access to disruptive technologies in the past was limited to few nations, individuals and institutions. It was easy to track who is doing what as developing any weapons of mass destruction required large amounts of money and infrastructure, and it was easy to track those. The technologies from cyberspace are not only accessible to everyone across nations, but they are affordable as well as it takes less than a thousand dollars for a computer. As a result, the power to create weapons of mass destruction in cyberspace or targeted destruction is now in the hands of masses.

Historically, the fear of any ground-breaking technology or technological transformation and its associated changes and challenges created calls for governments to regulate these new technologies responsibly. Each of these emerging technologies from cyberspace are dual-use in nature and can be misused. They can also behave in unpredictable and harmful ways towards humanity and could put human civilization at risk. While the dual-use nature of technology is nothing new, regulating emerging technologies like artificial intelligence, quantum technologies, gene editing, and more is an entirely different kind of challenge.

As seen, there is no clear global consensus on how to effectively govern the emerging technologies or their impact. Due to the fear of the free flow of information in cyberspace, nations are moving towards protectionism. Since decision-makers are still not sure of the path forward for possible ways to regulate the impact of emerging

technologies, many are choosing the more instinctive path of closing digital borders to prevent the negative impact of cyberspace technologies. While we do see positive efforts to discuss ethics and privacy, a much-needed dialogue on security implications remains notably absent in the governing equation.

To come up with effective regulations, there is a need to understand the security risks of each technology. Understanding the security risks will help nations move towards a security-centric approach to a technology regulatory framework. The bottom line is any regulatory policy for emerging technologies should be security-centric to be effectively controlled and governed. The need for a governance system that can be accepted by each nation and be easy to implement is also essential. While the nature of regulation has been discussed from adaptive regulation to sandbox regulation to outbox regulation, what is necessary is a security risk-centric regulatory and governance approach.

5. Natural And Human Made Environmental Disasters

From hurricanes to cyclones and tornadoes to natural and human-made wildfires, tsunamis and floods, droughts and more, disasters are growing in number, size, strength, and impact. While we have always faced natural disasters, we are currently observing a scale of disaster and destruction that is deeply concerning. Reports are emerging of disasters 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 caused by human pollution and activity, which contributes to these harsher disasters.

Furthermore, many human actions also may play a role in triggering some natural disasters like floods. For instance, rapid and unplanned urbanization of flood-prone regions increases the likelihood of floods. When water cannot get absorbed by the soil anymore, it keeps collecting and rushing down, creating bigger floods. Since a significant number of people live in such flood-prone areas, it increases the economic and security risks for nations. As a result, we must evaluate what role we humans play in environmental disasters.

As the number of natural disasters increased steadily over the last few decades, we must question whether the earth is becoming a dangerous place to live. At this point, nations lack the answers they need to solve the puzzle of natural disasters. The reason is perhaps the science of the earth and its environment is complex, under-evaluated, and still needs to be adequately understood. Amidst the complex challenges of our planet's environment, managing these growing disaster 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. As a result, there is a need for collective effort, initiatives, and investment in ensuring we use the collective intelligence of our species and the

technologies we have developed to protect our planet. It is time to apply collective intelligence to save our ecosystem.

6. The Integrity Of Information And Mass Manipulation Of Human Minds

Information is a critical dimension in today's asymmetric hybrid warfare as the boundaries between information and intelligence are blurring rapidly.

As seen, controlling minds and manipulating human behavior through social media seems to be on the rise. For instance, any tweet can go viral without any fact checking, seen in the ongoing 2019–20 Wuhan coronavirus outbreak. The integrity of information that can be seen in most viral messages is deeply troubling. That brings us a question of whether cyberspace platforms are increasingly used for misinformation, disinformation, and invisible psychological warfare to manipulate public opinion.

Moreover, information obtained through a data breach and from personally identifiable information is also increasingly used for malicious purposes. With the advances in mind control technologies and brain-computer interfaces, the opportunity for malicious use of the brain-computer interface will also likely grow in the coming years.

Most individuals today do not have the expertise, skillset, and resources to evaluate the integrity of information; as a result, they are vulnerable to today's misinformation and disinformation campaigns growing in cyberspace and will be in the coming tomorrow as well.

Since knowledge is the source of power, not having credible information weakens the strength of informed decision-making. It is, therefore, essential for everyone to acquire new skills and competencies to differentiate credible information from the onslaught of misinformation and disinformation. Perhaps this is something schools should teach all of its students from a young age.

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. If left

unchecked, a lack of information integrity and the erosion of facts will ultimately contribute to society's collapse.

A lack of information integrity is a critical security risk facing humanity. We must, therefore, develop the necessary tools and techniques to avert this decline.

7. Social Isolation, Loneliness, And Mental Health

Loneliness or a state of chronic perceived social isolation in all age groups is a growing global health and security problem. The reason is that humans are social creatures. It is the social connection and interaction that enables everyone from our species to progress, thrive, and survive. According to an NIH report, social isolation and loneliness are related to health problems such as cognitive decline, depression, and heart disease. This has also been documented by the late Dr. John Cacioppo's research that underscored that 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 worse.

Considering our origins as a tribal species, we did not get here overnight to a world moving towards isolationism and social isolation. A range of factors have contributed to loneliness today, and one of the critical variables is technologies from cyberspace.

Moreover, professional lives are increasingly transient. Uprooting our lives for a job opportunity to different geographical locations is proving to be very difficult for many. Furthermore, the rise of remote working, while offering flexibility, meaningfully reduces social interactions. Outside of work, meeting new people can be a struggle for many, as we have few shared community institutions and initiatives. Stress levels show no sign of abating, and technology has reduced our need for in-person interactions. People of all age groups, including our senior citizens, increasingly live and age alone. This is just the beginning.

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 human connections, connectivity, and relationships are fundamental 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, purpose, and productivity will be the new norm.

While social isolation and loneliness do not necessarily go together, it is essential to understand whether they are independent processes or whether they have interdependencies. Irrespective, it is crucial to understand that everyone needs to engage in meaningful and productive activities to live a life that is fulfilling. As nations are accountable to its citizens irrespective of their background, class, age, and state to a life that gives them a purpose and meaning, it is time we put our collective efforts in solving this critical security risk facing humanity.

8. Rise Of Infectious Diseases, Pandemics And Nation Preparedness

The global health system has come a long way to protect and promote human health. Despite that, we at the moment are on the verge of a pandemic, the large-scale 2019–20 Wuhan coronavirus outbreak.

The World Health Organization (WHO) has declared the Wuhan coronavirus a global emergency. As a result, the potential of economic, social, and political turbulence is imminent. Reports are emerging of Russia closing its border to China. Airlines have canceled their flights to China. The fear of the looming healthcare threat to individual countries is setting in as a large number of people seem to be needing hospitalization in China, and the system seems to be not keeping up. While China is trying to build more hospitals to keep up with the growing needs, the reality of the Pandemic Preparedness is raising more questions than answers. Are nations ready for the Coronavirus driven pandemic? Do we have effective medicine and healthcare supplies to meet the emerging need? Are nations prepared for any virus centered pandemic?

While a virus drives this on-going crisis, pandemics can also be caused by bacteria and fungus as well. Although antibiotics have been effectively controlling many bacterial infections and there are some treatment options available for viral diseases, there are not many treatment options available for fungal infections. Antibiotic resistance is a growing concern as well. Since increased global travel and integration has increased the possibility of more pandemics, we need to evaluate what is necessary for national preparedness for a pandemic of any origin, class, mode, and intensity.

In recent memory, we have witnessed the 2003 SARS (severe acute respiratory syndrome) epidemic, multiple Ebola outbreaks, and the 2015-16 Zika epidemic, to name just a few. There is a need to embed preparedness and increased healthcare capacity into all our systems across nations – especially for the timely identification of disease, quarantine procedures, and communication and control, to provide primary care to everyone. There is also a need for better preventive and therapeutic drugs.

The increasing emergence of viral diseases from animals is a significant concern. At the same time, there is also a potential of human originated outbreaks emerging from laboratory accidents or even intentional biological attacks. Amidst that, the looming threat of rising antimicrobial resistance is also adding to the growing concerns. It is time to collectively focus on how to address the risks of emerging pandemics.

While there is growing uncertainty to pandemics and their impacts, the reality remains that outbreaks will continue. The question is, are nations prepared for what could come?

9. Declining Civilization Thinking And Rise Of Tribalism

It is said that humans are tribal animals and need to belong to groups. While the digital age was supposed to increase civilization thinking, the rise of tribalism is underscoring the failure of information and communication technology to close the divide of the human population based on nationality, class, color, religion, and sex.

Over the years, many have become used to standing on their own, living life based on their independent thinking and not being concerned about tribes or communities. It seems that stand and approach seem to be in decline. The geopolitics of cyberspace is a perfect example of the growing power of tribalism. The unending wars of the Middle East based on theology or ideologies, involving countries around the world, are another glowing example of the rise of tribalism.

While the idea of tribalism gives comfort and a false sense of security, tribal loyalties are destructive and will most certainly negatively impact the future of humanity. History has shown numerous examples of the negative impact of tribalism on nations' progress and development. From the Balkans to Northern Ireland, Beirut, Myanmar, and more, nations have witnessed horrifying tentacles of tribalism making neighbors kill neighbors. Religion-based tribalism is on the rise in India. Even now in the United States, the so-called melting pot of nationalities, tribalism based on political ideology has intensified and is taking an ugly turn.

It needs to be understood that tribalism is a destabilizing force as it not only discourages thinking and individual decision-making but also forces loyalty to something that looks backwards and not forwards.

While tribal cohesion was essential to survival for nations over the years, in the digital age, as we create artificial intelligence and begin to dream of exploring the universe, the question is whether nations should think and act as a single human species or in silos as different tribes. How we represent our species will influence the development of artificial intelligence also, and what comes next in our collective journey will entirely depend on whether we act as a cohesive civilization.

When, even today in the digital age, the identities that matter most are based on ethnicities, religion, or sectarian or class-based differences, it is a cause of great concern and a security risk for the future of humanity.

10. Collapsing Systems And Economic Uncertainty

We are living in an age of intense turbulence. Geopolitical tensions are deepening. The technologies from cyberspace are overturning long-held assumptions about security, geopolitics, economies, and society. The long-held notion of political parties and political ideology are in crisis as well since they continue the governance model approach based on left or right, capitalism versus socialism, and outdated goals and issues. The reality is that the core issues of political parties seem to be outdated.

Technologies from cyberspace are forcing the redesigning and redefining of systems as the current governance systems are not keeping up with the impact of the technological transformation. On-going cyber breaches and the onslaught of regulatory challenges are making the current systems vulnerable to disruption and collapse. As seen, the financial system is collapsing. Bank jobs are dwindling as bank branches are closing due to banking moving online. The same is the situation with commerce as consumers are rushing to online stores over retail stores for their shopping needs. This is just the beginning.

Now a cyber-attack can cause the next financial crisis. A cyber-attack can also cause an energy crisis, transportation crisis, or crisis of any digital system. The reality is that all connected systems are at risk from cyber-attacks. This is just one driver of the on-going collapse. We are also witnessing global trade collapsing due to many other reasons. The supply chain is shifting. Also, the rapid advances in artificial intelligence-driven automation adoption by industries are collapsing the traditional way of doing things and systems. Every industry is at a threat from AI-driven automation. Moreover, 3D printing, digital additive manufacturing, synthetic biology, and in the coming years molecular manufacturing, will further collapse the systems. Furthermore, asteroid mining and space mining will create new supply chains for nations, thereby collapsing more systems and ways of doing things.

The interconnected and interdependent systems are increasing the vulnerability of the global systems. Individually and collectively, each of these variables and more play a role

and will play a role in the collapsing systems. As a result, due to rising unemployment, shifting supply chains, and vulnerability to cyber-attacks and more, economic and security uncertainty will be on the rise across nations.

Nations with a proactive integrated security risk management framework will be able to resist the shocks of the systems. Nations with effective change management processes will be able to transition to emerging systems without much turbulence. It is, therefore, crucial that each nation defines how to survive in an age of uncertainty.

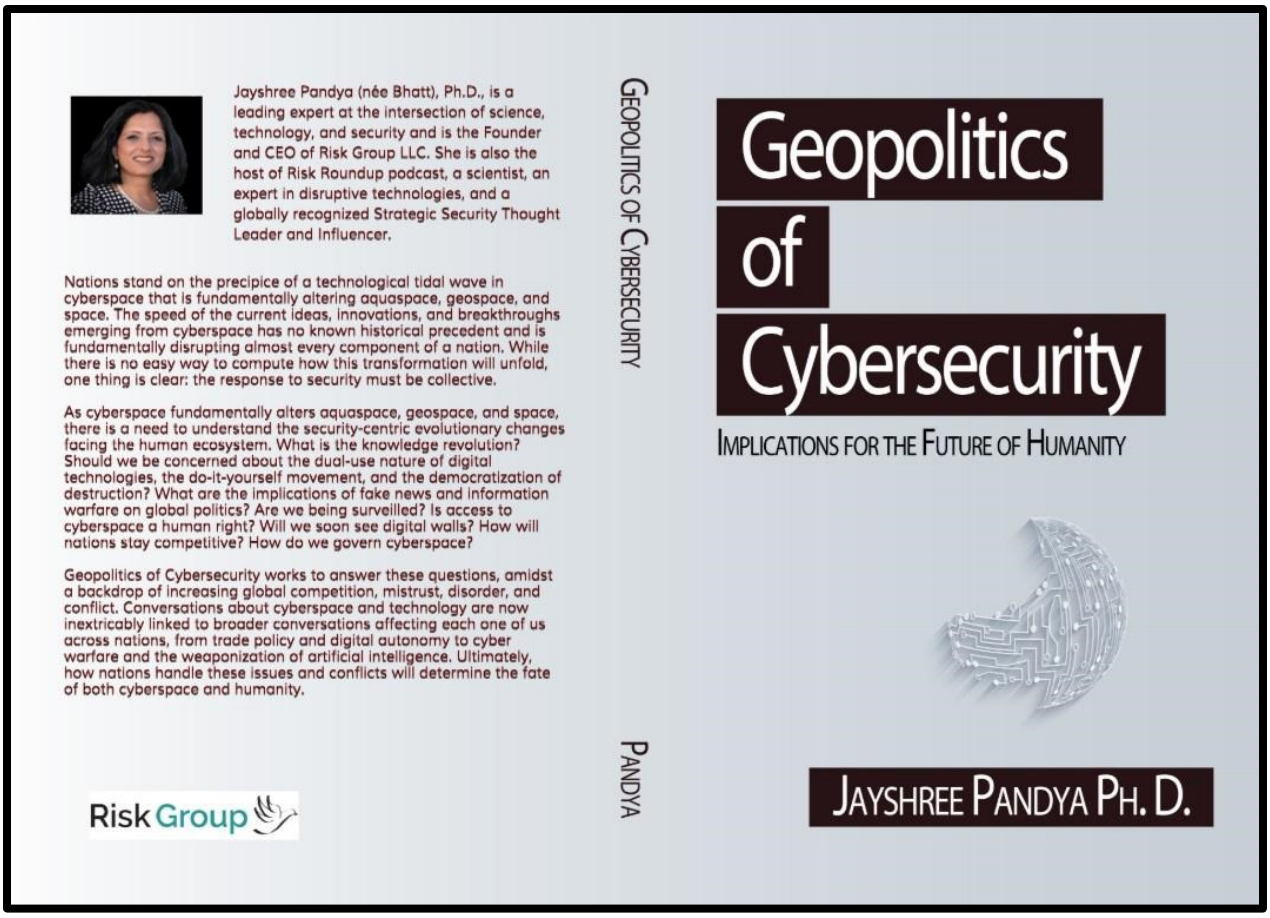
If nations are to survive this age of turbulence and complexity, it is essential to understand the on-going technology transformation, what it means for all components of a nation, and how to navigate the complexity of the economic and security turbulence.

Conclusion

While we have briefly discussed the top ten strategic security risks facing humanity, many other strategic security risks also need serious attention. From autonomous systems to distributed systems, quantum technologies to a technological singularity, disappearing jobs to the loss of wages, and mass migration to social unrest, there are many emerging strategic 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.

While over the years, we have survived looking at the short-term risks, we are now living in an age where it is critical to have a long-term view of the strategic security risks emerging that could negatively impact the future of humanity. We not only have to understand the strategic security risks ourselves but also have to teach them to one another and embed this strategic security risk thinking ability in our future generations if we are to survive as a human species. There is no doubt that the coming years are going to be highly turbulent. It will require strategic thinking ability and analytical capabilities. We will need to learn to adapt and manage complex changes and solve complex security problems. Moreover, we need to be resilient and develop resilient systems to face the emerging systemic shocks.



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

Jayshree Pandya (née Bhatt), Ph.D., a leading expert at the intersection of science, technology, and security, is the Founder and Chief Executive Officer of Risk Group LLC. She is also the host of highly influential Risk Roundup: Podcast/Webcast, a scientist, an expert in disruptive technologies, and a globally recognized Strategic Security thought leader and influencer.

Dr. Pandya has been involved in a wide range of research, spanning security of and from science and technology domains. Her work is currently focused on understanding how the converging technologies and its interconnectivity across cyberspace, aquaspace, geospace and space (CAGS), as well as individuals and entities across nations: its government, industries, organizations, and academia (NGIOA), create survival, security, and sustainability risks. This research is pursued to provide strategic security solutions for the future of humanity.

Dr. Pandya's passion for solving complex problems facing humanity using science and technology began during her childhood. She pursued her interests in her studies, and in the 1990s, while doing her doctorate, she developed a Hydrogen Production system using Halobacterium halobium. She also developed a desalination process and discovered anticancer drugs. The trends continue as she gets actively involved in developing numerous solutions to complex problems facing humanity.

Over the years, Dr. Pandya has made significant contributions to the fields of Microbiology, Biochemistry, Anti-Cancer Drugs, Bio-Energy, and more. Her work on the technology layers of cyberspace encompasses the needs of Cyber-Security and Global Security, including defining the Interconnectedness of the Human Ecosystem (an integrated CAGS security framework). Dr. Pandya has also proposed a need for an Integrity Rating System of Algorithms (a theory for integrity of news and online content), an Algorithm Naming and Identification System (a framework to identify and track algorithm that brings security risks to the future of humanity), and most recently, the need for redefining the role of insurance to be the enforcer of risk management systems across NGIOA and ensuring a clear set of rules and model to manage the interconnected and interdependent security risks from the human CAGS ecosystem.

From the National Science Foundation to organizations from across the United States, Europe, and Asia, Dr. Pandya is an invited speaker on emerging technologies, technology transformation, digital disruption, and strategic security risks. Her work has contributed to more than 100 publications in the areas of science and commerce and has garnered her many advisory position honors. Her latest book, Geopolitics of Cybersecurity, offers much-needed solutions to the rising digital disorder.