GLOBAL RISK INTEL

DOMINANT RISKS IN THE DEFENSE & SECURITY INDUSTRY

2019

www.globalriskintel.com

DOMINANT RISKS IN THE DEFENSE & SECURITY INDUSTRY

2019

Global Risk Intelligence

APRIL 11, 2019

Washington, D.C. · London · Dubai · Singapore

www.globalriskintel.com

DISCLAIMER:

THE VIEWS EXPRESSED IN THIS DOCUMENT ARE THE SOLE RESPONSIBILITY OF THE AUTHOR(S) AND DO NOT NECESSARILY REFLECT THE VIEW OF GLOBAL RISK INTELLIGENCE. THIS DOCUMENT IS ISSUED WITH THE UNDERSTANDING THAT IF ANY EXTRACT IS USED, THE AUTHOR(S) AND GLOBAL RISK INTELLIGENCE SHALL BE CREDITED, PREFERABLY WITH THE DATE OF THE PUBLICATION.

About Global Risk Intelligence

Global Risk Intelligence is a boutique risk advisory firm which provides consulting services to anticipate, assess and advise organizations. We utilize data to drive critical and confident decisions. We provide risk management training at all levels -enterprise, country and project specific. We identify, assess and evaluate risks, as well as opportunities, in existing operations. We monitor potential threats that impact operations, strategy and reputation.

Why Global Risk Intelligence?

We are agile and flexible – we are ahead of the game with responsive innovation. Global Risk Intelligence embraces new ideas and anticipates and responds to changing customer and market opportunities.

We are collaborative and thrive on strategic partnerships and alliances. In this current world, where accurate data and information is at a premium, people need to be able to rely upon an advisor that is gather sufficient, reliable information, analyzing this information and making articulate decisions.

Gain a Competitive Advantage

We DIVE DEEP – there is a true depth of research by our PhD and higher educated subject matter experts located globally. We offer detailed analysis to executive teams to assist in shaping business decisions.

Authors

David Hutchins, MSc is a Risk Analyst at Global Risk Intelligence. He earned his MSc in Defence, Development, and Diplomacy with Merit from the Durham Global Security Institute at Durham University. He maintains 6 years of military experience and serviced in the United States Marine Corps Forces Reserve.

Justin Marinelli, MSc is a Risk Analyst at Global Risk Intelligence. He earned his MSc in Global Politics from the School of Government and International Affairs at Durham University.

Alexander Hutchins is a Risk Specialist at Global Risk Intelligence, where he focuses on cybersecurity issues. He has competed in a number of cyber defense competitions and simulations. Aside from his technical expertise, Alexander maintains experience in the pharmaceutical sector.

Note from the President & CEO

Although risk is an ever-present element, it is certainly not constant in its forms and can assume innovative and threatening positions within the defense and security industry. Damage can at times be devastating or even irreversible. Regardless of the degree however, risk is to be evaded. Therefore, it is crucial to be aware and keep abreast of current and forthcoming risks.

While 2019 presents a volatile global order, layering risk has further complicated its dimensions of intricacy. As technology advances, industry dependency on cutting-edge responses simultaneously grows. Certain situational developments may indeed present alarming scenarios, such as sales and deployments of highly advanced defense systems. It should also be noted though that invulnerability is never guaranteed for any party.

Global Risk Intelligence is proud to present this report, which recognizes five dominant risks in the defense and security industry. Through the overarching risks, the interconnectedness of the international system has been emphasized coupled with vivifying the tangibility of globalization.

Dr. Nadir Gohari

President & CEO

Contents

Introduction

For companies involved in the defense and security industry to maintain best practices, it is essential to stay up-to-date with the latest industry risks. Rapid technological advances to the defense and security industry, threats of cyberattack, an increasingly competitive global market, and volatile geopolitical tensions have all created dynamic challenges to countering emerging threats. There is no doubt that 2019 will see the continued evolution of threats to this industry and will therefore require the necessary foresight and precocious measures to counter such threats. Proper management and mitigation of risk requires an elevated state of readiness. Therefore, the defense and security industry has a definite need for a highly skilled, expertly trained, and well-equipped workforce that is acquainted with the latest industry risks. The following risks presented in this report have been selected based on thorough analysis of factors that will continue to generate risk in the coming year.

Emerging Technologies

With the continued integration of next-generation technologies into the defense and security industry, it is absolutely essential that those seeking to mitigate risk stay acquainted with cutting

edge innovations in technology. The inclusion of unmanned technology, advanced robotics, and artificial intelligence into the defense and security industry has resulted in a rapidly changing landscape that necessitates self-refining practices. The defense and security industry of the near future must strive to implement the latest hardware and software while maintaining personnel that can effectively operate them. Moreover, the use of technologies like cloud computing and machine learning can be used to

improve communication and logistics and augment both the testing and practical application of operations.

While a vast array of technologies play a role in the defense sector, a few critical emerging technologies to monitor are as follows:

- Unmanned Systems: Further development of unmanned systems will be a key driver of risk in the defense and security sector in the coming year. The flexibility of such systems allows for multi-varied use not only by state-level militaries, but also smaller non-state forces. Technological advances in areas such as autonomy, network integration, and stealth will primarily accrue towards highly advanced state-level militaries, but less advanced entities using more basic systems will still be a driver of risk in this area. Asymmetric forces will seek to use such devices in unorthodox ways to achieve tactical ends. Among other things, this means that the risk of a terror attack carried out with the aid of unmanned systems is a key threat.

- Artificial Intelligence: Advancements in artificial intelligence (AI) will enable faster, more efficient processing of massive amounts of data. While this on its own offers a security advantage, it will also open up new possibilities for both tactical refinement and technological development. In addition, the further sophistication of AI in the cybersecurity realm will be an important factor driving innovation in cyber-defense. However, the risk of AI systems being used for the purpose of malicious cyberattacks is increasing as well and AI offers significant potential for heightening the effects of disinformation campaigns and other psychological operations.

- Stealth: Breakthroughs in stealth technologies have been integral to the development of 5th-generation fighter jets. As more nations work to develop their own stealth aircraft, further progress is to be expected in this area. Countries such as China, Russia, and Turkey are all seeking to develop their own 5th-generation fighters. Moreover, stealth countermeasures are being pursued by nations, like Russia, which hopes to be able to successfully combat stealth aircraft with new technologies such as its upcoming S-500 missile system.

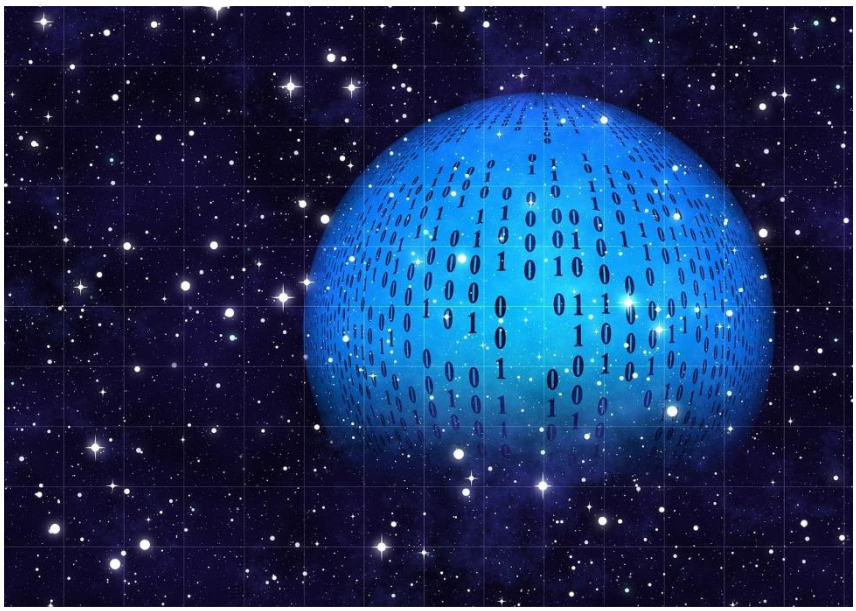
- Space-Based Platforms: Proliferation of space-based assets will yield new dimensions to security conflicts. Existing Command, Control, and Communications (C3) capabilities will continue to be augmented by the placement of new satellite systems and the efforts of new actors to acquire these capabilities will accelerate the development of space for security purposes. Major powers will continue to develop anti-satellite capabilities to combat rivals in the space domain, which will also exacerbate competition in this arena.

Cybersecurity

The global trend of increasing dependency on computers, cloud-based systems, and interconnected networks has made cyber security progressively more important. It is absolutely crucial that those involved in the defense and security industry be aware of the current cyber warfare capabilities and its potential future applications. The growing reliance on computing systems for business operations creates a concurrent vulnerability to cyberattack. Therefore, defending against this risk is increasingly important. Not only has the number of cyberattacks worldwide risen in past years, but also the degree and severity of attacks. It is estimated that the global total value of funds lost to cyberattacks in 2017 was $600 billion USD. This profound number is expected to reach $6 trillion USD by 2021. From a defensive standpoint, each business in this industry should apply the latest cyber security measures, and at a bare minimum, should be aware of what cyberattacks may target their operations. Large companies have been regularly attacked in various industries, leaving an enormous amount of sensitive data at risk.

As recent history demonstrates, hybrid warfare between governments and the practice of state-sponsored cyberattacks are increasingly more common and preferred over direct conflict, especially in the developed world with competing industries. It is easy to understand the appeal of conducting state-sponsored cyberattacks as opposed to military action, given its extreme effectiveness with virtually no risk of casualties. This type of warfare allows a small group of specialists to operate covertly behind the wall of national sovereignty enforced by military protection. Each of the world's most powerful governments possess advanced cyber warfare capabilities. This includes traditional adversaries to the United States including Russia, China, Iran, and North Korea. Most notably, Russia and China have invested heavily in this new type of warfare,

allowing them to gain a more balanced stance with the United States on the stage of global power competition. Therefore, the defense and security industry must be well prepared for this type of assault in the coming year.



Additionally, operating within the defense and security industry allows for the opportunity to consider offensive capabilities of cyber warfare. When considering the most effective tools for achieving mission success and reducing damages or casualties, using the most innovative technology has naturally demonstrated to be advantageous. Possessing an elevated understanding of the threat that cyber warfare represents and knowing how to capitalize on its utility will be a valuable asset in the coming year.

Indeed, the recognition of and counteraction to all forms of cyberattacks is essential for those in the defense and security industry. Those targeting computer systems, networks, or personal devices can employ a variety of methods to steal, alter, or destroy information. This includes attacks such as disk operating systems (DOS), phishing, Structured Query Language (SQL) injection, password attack, cross-site scripting (XXS), eavesdropping, and malware.

Supply Chain

The interconnectedness of the global supply chain ensures that defense and security organizations face massive exposure to a full suite of supply-chain risks. Supply-chain vulnerabilities affect every part of the procurement process and defense organizations are particularly vulnerable to supply chain manipulations due to both their procurement needs and the sensitive nature of the issues they address. Product defects arising from supply chain vulnerabilities have the potential for consequences of enormous magnitude. Counterfeit parts, substandard components, or sabotaged materials all undermine the capabilities of defense products and can even lead to penetration by malicious actors.

The threats to supply chain integrity cover an array of challenges, from counterfeit or mislabeled parts to breakdowns in operational processes to deliberate attacks by malicious actors. The consequences from these threats vary in magnitude. Mislabeled parts may not meet required specifications and may fail to perform in critical conditions. Operational breakdown may cause delays in procurement timelines and production schedules. Finally, penetration of the supply chain process by malicious actors can induce vulnerabilities that cannot be mitigated by cybersecurity best practices or other risk management techniques. Once such an operation has been successfully completed, it cannot be mitigated except by a re-procurement of unaffected components.

A controversial Bloomberg article[1] positing sabotage of microchips sourced from China has been neither proven nor disproven, but its suggested narrative highlights the potential dangers of a

[1] **Robertson, J. and Riley, M. (2018). "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" in *Bloomberg Businessweek*. Available online: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (Last Retrieved: April 10, 2019).**

state-level actor inducing vulnerabilities in the supply chain process. Concern over the possibility of such an operation has been part of the impetus behind a renewed US Government focus on supply chain security. Organizations working in the defense and security sector are advised to weigh similar concerns about the sourcing of critical components and materials.

Similarly, the use of mislabeled parts also pose grave concerns. Manufacturers desperate to cut costs have incentive to replace key parts with similar, but lower-quality components. This type of scenario is more likely to occur in places with fewer institutional measures for the regulation of quality control. The ultimate effects of such mislabeling will look similar to intentional sabotage and could have similar results.

The processing of certain materials, such as cobalt or rare earth minerals, also presents risk to supply chain integrity. Given the limited number of locations at which certain key strategic resources can be accessed, the supply chains for requisitioning these materials are more vulnerable to disruption. For example, volatile or unpredicted events such as political disruptions or natural disasters, respectively, can also have a potentially tremendous impact on access to such resources. Certainly, this can affect critical operations or procurement processes.

Remedying such potential vulnerabilities requires serious and comprehensive assessment of supply chain risk. The supply chains for the advanced technologies used in the defense sector stretch through thousands of miles and over numerous stages. Auditing of such interconnected processes is extremely difficult, costly, and time-consuming. Prototypes of models for wholesale supply chain assessments are being developed now and the urgency of the matter has led to such research being done at a rapid pace. However, these primordial efforts highlight the difficulty of maintaining integrity within global supply chains.

The defense and security sector relies on the most advanced technological equipment in order to achieve its goals. Vulnerabilities in defense sector supply chains can undermine the capacity of key technologies to fulfill their purpose. Given this area of risk, proper supply chain management is integral to organizational risk management. Congruent error-free processes that include system interoperability assessment are just as important as possessing the latest in advanced technologies.

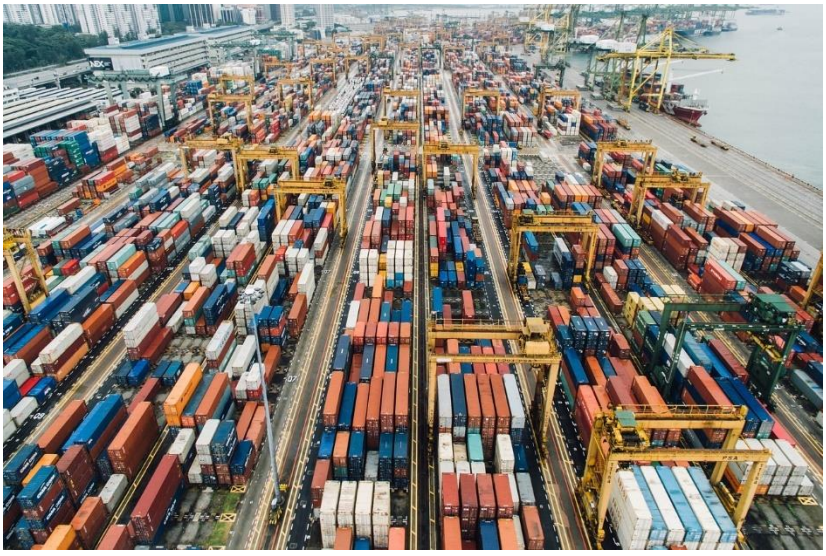
Rise of International Market Competition

Global arms trade has been rising steadily since 2002, now with just ten countries accounting for 90% of the market. The United States maintains its position as the global frontrunner accounting for 34% of global arms exports between 2013 and 2017. However, the global arms trade is witnessing a gradual but significant shift away from the traditional US-centric market. Russia has risen to contest the US, making itself the immediate competitor. China is also moving to compete in this field, appearing as the more long term competitive threat. The two most significant increases in arms exports between the benchmarks on 2008 – 2012 and 2013 – 2017 came from Israel and China, which saw a sales increase of 55% and 38%, respectively. The arms trade industry of these two countries is rising at a faster rate than that of the US, with China possessing the capability to rival the US in the not-so-distant future. Rising powers like Russia and China becoming increasingly involved in the global defense and security markets will result in a more competitive global market and require improved cost effectiveness, superior products, or both in response. Chinese manufacturing and Russian weapons development companies are just two examples of rising industries that will compete with the American market in 2019.

Despite having experienced a decrease in arms sales between 2008 – 2012 and 2013 – 2017, Russia still represents a strong arms trade competitor to the US as the second largest arms exporter in the world. A perfect example of Russia's ability to compete with American manufacturers is their sale for the S-400 surface-to-air missile defense system to Turkey. A longstanding ally and NATO member, Turkey traditionally purchase weapon systems from the US or its allies. However, Turkey chose to purchase a Russian-made system over American-made alternatives. This trend has

continued with other countries to include China and India. Market competition from Russia has demonstrated their ability to provide highly functional weapons systems at low costs.

Moreover, China has proved itself as a world leader in manufacturing and will likely continue this trend by investing further into the industries of defense and security. China's control of critical materials such as rare earth minerals needed for manufacturing products in the tech industry provides an additional challenge to the global defense industry. Without diversifying methods of acquiring the necessary materials, there exists a significant risk to the production of next generation technologies. China maintains the ability to limit access to vital materials within the supply chain, thus demonstrating the risk of foreign dependency.



While Russia and China might represent the biggest rising threats in the international market, Europe is also home to many powerhouses in the arms manufacturing industry. Combined, France, Germany, Spain, Italy, and the United Kingdom (UK) accounted for almost one quarter of global arms sales between 2013 and 2017. With companies like France's Thales, Italy's Leonardo (formerly Finmeccanica), and the UK's BAE Systems, long-established allies will be competing between each other for some contracts. It is also worth noting that France is the world's third-largest arms exporter behind the US and Russia.

Current events surrounding the relationship between the US and the Kingdom of Saudi Arabia threated to substantially decrease US arms sales and thus could cause the world's second largest customer to look elsewhere for its weapons needs. US President Donald Trump and his administration has come under mounting pressure to suspend arms deals with Saudi Arabia, which is currently the number one recipient of American arms sales. US arms exports to Saudi Arabia had

previously increased by 448% between 2008-2012 and 2013-2017[2]. A reversal of this trend would impact US arms exports a great deal and allow for other nations to capitalize on Saudi Arabia's demand for weapons.

Another factor affecting the international market is the development of indigenous arms programs. For example, some key weapons customers such as Saudi Arabia, Turkey, and India are investing more in their indigenous arms development programs. While still currently investing in foreign arms trade, the aforementioned countries are developing their own arms industries which may significantly reduce their dependence on foreign arms sales in the coming years.

[2] **Statistical figures obtained via Stockholm International Peace Research Institute (SIPRI). Available online: https://www.sipri.org/sites/default/files/2018-03/fssipri_at2017_0.pdf (Last Retrieved: April 10, 2019).**

Geopolitical Volatility

As the world market becomes increasingly more globalized, events that affect markets elsewhere can have ripple effects across the globe. While today's globalized market allows for large multi-national projects to transpire with relative ease, this interconnected nature can result in detrimental effects when facing issues such as trade wars between global powers. Rising international market competition coupled with heightened political tensions has generated numerous trade disputes. These disputes could very-well lead to trade wars in the coming year, especially between the United States and its competitors. The subsequent tariffs could target materials needed by the arms industry, and therefore increase the cost of production. While much of this risk depends on political uncertainty in the coming year, it would be considered best practice to prepare for the impeding effects that trade wars could have on the industry.

This globalized market requires persistent attention to the fluctuating geopolitical relations abroad. For example, faltering bilateral relations could place ongoing projects at risk. On the flipside of this issue, geopolitical volatility could result in conflict that requires solutions from the defense and security industry. Staying ahead of these risks and remaining aware of the geopolitical tensions at play will allow for one's company to remain prepared for the aforementioned risks.

The international market has become interdependent, therefore escalating trade disputes between the United States, China and many of the United States' traditional allies will undoubtedly have both direct and indirect consequences relating to the defense and security industries. Moreover, military tensions will remain high between the United States and China until both nations resolve their political and economic differences. Should the relationship between the US and China continue to sour, American defense industries could miss out on contracts with the world's 5th

largest arms importer. Along a similar trend, India represent a sizeable potential for defense industry sales as this nation is the world's top arms importer. However, as of 2017, India has received 62% of its arms from Russia and only 15% from the United States.

In summary, geopolitical volatility constitutes a serious threat to the defense and security industry given the impact that heightened political tensions has had on international trade. In the coming year, companies in the defense and security industries may find it more difficult to acquire the materials necessary for manufacturing or to maintain positive relations with clients abroad. Geopolitical volatility and the subsequent disputes that arise can lessen mutual trust between nations and can therefore be detrimental to the overall industry.

Contact Global Risk Intelligence

To discuss values, explore options, or obtain additional reports, please contact us at our Washington, D.C. or Arlington location:

Jennifer Hoffman

Senior Vice President, Business Development

jhoffman@globalriskintel.com

1717 Pennsylvania Ave. NW
Suite 1025
Washington, D.C.
Tel: +1 (202) 981 – 5972

1220 N. Fillmore Street
Suite 400
Arlington, VA
Tel: +1 (703) 988 – 5954 Ext. 5905

For further information visit www.globalriskintel.com.

americas@globalriskintel.com
Washington, D.C.

europe@globalriskintel.com
London

dubai@globalriskintel.com
Dubai

asia@globalriskintel.com
Singapore

Notes

www.globalriskintel.com