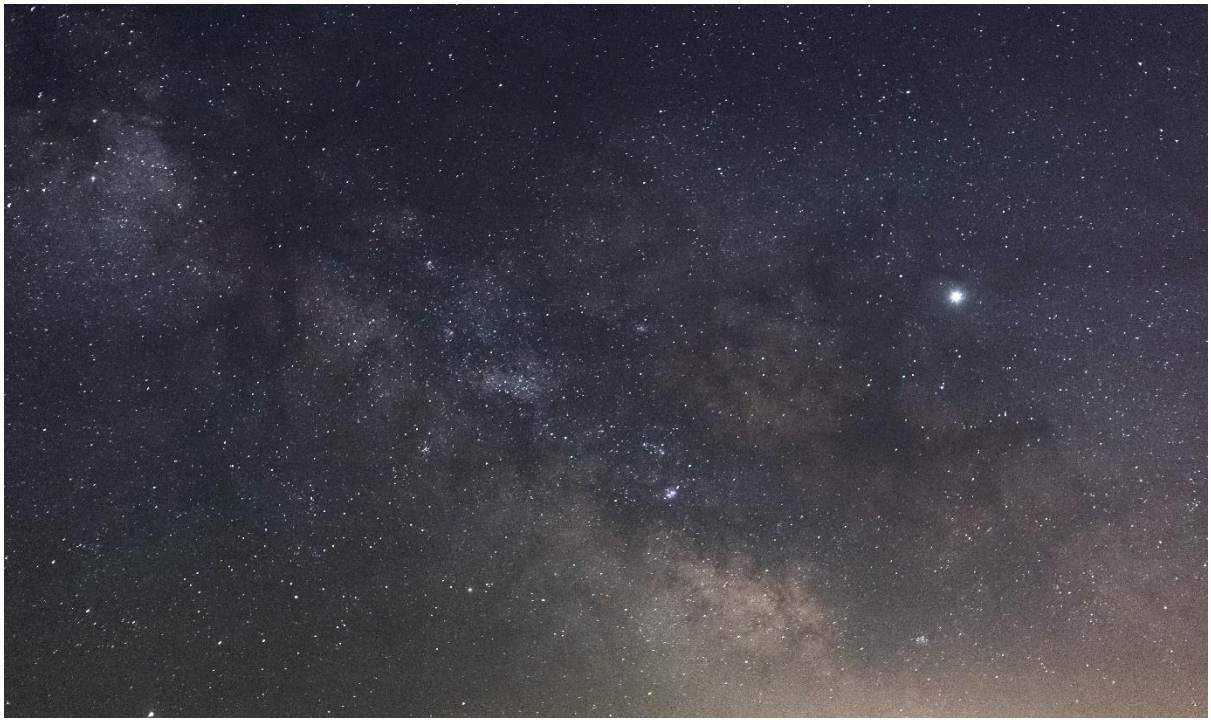
3 disruptive frontier risks that could strike by 2040



"Outer space is becoming increasingly congested, contested and competitive."

18 Dec 2020

Nayef Al-Rodhan

Honorary Fellow, St. Antony's College, Oxford University

- Bio-hazards, cyber-crime and space conflict all pose major risks over the coming decades.
- International cooperation is key to prepare for these threats.

Our world is becoming increasingly interconnected and interdependent due to the unprecedented exponential growth of various transformative technologies. This carries significant benefits but also some risks. It will be our duty to harness our progress towards combating and mitigating these risks.

Three major and likely frontier risks stand out in particular over the next two decades.

1. The next bio-catastrophe

Perhaps the only silver lining arising from the Covid-19 outbreak has been its propensity to better prepare us for a future pandemic, which might well involve a much deadlier pathogen, and to highlight the gaps in our present understanding and capabilities.

Worse still has been the distinct lack of cooperation between states in tracking and tracing the virus, and in sharing information. The fact that a pandemic is global by definition has not stopped some governments insisting that information should remain national or regional at best.

However, were we in the future to face a virulent pathogen (spontaneous or man-made) – likely to be much more dangerous – the issue of locating its origins and stifling its spread would not just be a public health priority, but a national and international economic, political and security crisis.

Next time we might require far more equipment than face masks and ventilators, and much better and quicker national responses and international cooperation to procure it. Significant national and transnational investments (public and private) in R&D for basic science research, therapeutics, vaccines technologies, and bioinformatics must be an urgent priority for all.

As soon as possible, irrespective of existing security measures for studying diseases and bioweapons, all governments must undertake serious reviews of what is being studied, and what its effects and potential risks are. As we've learnt, before thinking of treatments or cures, the chief areas of concern with any new pathogen relate to determining its origin, fatality levels, transmissibility and tracing.

Protocols for international cooperation between governments and corporate sector on future pandemics, biohazards, and relevant progress, should be reviewed annually, at a specially dedicated conference at the United Nations. Methods through which the private sector can harness its innovations and contribute its available resources, through collaborative public-private sector partnerships, should similarly be prioritized at major policy gatherings such as the World Economic Forum.

2. Cyber-meltdown

The second sphere which we should focus on is that of major cyber threats. Potential disruptions may include major cyber-financial meltdown, critical infrastructure collapse, or nuclear or bio facilities disruption. These could be triggered by rogue states or non-state actors and could have major and serious consequences.

Another pertinent trend related to cyber security concerns is the sharp rise of supply chain attacks.

The international cybersecurity agenda focuses on developing norms for responsible state behaviour, capacity building, the application of international law to cyberspace, and confidence building measures. Drawing on this, we can identify four general principles that guide the international discussion on cyber security.

First, the central importance of national sovereignty as the basis for State responsibility in cyberspace. National sovereignty firmly embeds cybersecurity in the existing framework of state relations under the Charter of the United Nations.

Second, the applicability of existing international commitments and law to cyberspace. This is the sphere in which there is more work to be done. We must necessarily update our international treaties and protocols to reflect the rapid evolution of cyber threats, as described above, and meetings to review enforcement priorities and capabilities must be held more frequently.

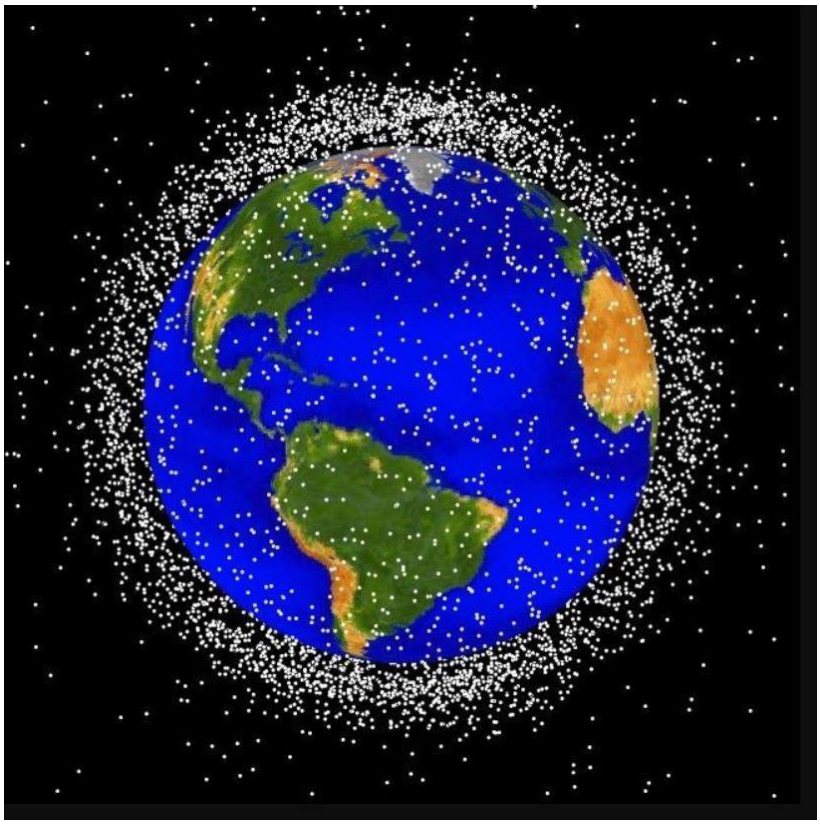
Third, acceptance by states of their responsibility for cyberattacks originating from their territory. It is crucial for non-state actors to feel the force of law of the jurisdictions in which they operate.

Finally, the need for a commitment by nations to cooperate with others and assist them in the event of a crisis. This amounts to a recognition that, while states must take responsibility for malicious actors within their borders, both the perpetrators and the recipients of cyber-attacks tend to be spread across borders.

3. Conflict in outer space

Outer space is becoming increasingly congested, contested and competitive. This is due to the exponential increase in satellites, private sector involvement, power politics, economic competition and the critical relevance of space to terrestrial affairs in peace and war.

Potential risks and conflict can result from two threats: 1) the exponential growth of Space debris and 2) the increasing militarization of outer space. In recent years, space has become increasingly contested, with public and private actors trying to assert their dominance, or attempting to harness the opportunities that outer space technologies and infrastructure bring for profit.



A NASA graphic showing space debris Image: NASA

Some 20,000 debris pieces roughly the size of a tennis ball are floating around, capable of rupturing spacecrafts. The number of active and dysfunctional satellites is increasing exponentially, as many states and companies attempt to launch tens of thousands of new ones.

The creation of "Space Forces" by many states is an ominous sign for the sustainable security of outer space, and competition rather than cooperation is the prevalent paradigm.

The use of ASAT (Anti-satellite) tests by major space faring nations has created a dangerous precedent and as a result produced large amounts of space debris, which is yet to be removed through serious cooperative technological and financial efforts.

Moreover, evidence of the militarization of space is growing by the day.

Humanity is becoming increasingly and irreversibly dependent on outer space for our daily lives, from civilian flights, mobile telephony, the Internet, rescue at sea, telemedicine, GPS, environmental and disarmament monitoring etc. States also depend on space-based assets and systems for military, security and diplomatic capacities, both in war and peacetime. The US-born global positioning system (GPS) has grown to be the most indispensable global system created by humans – providing the base for the rest of the world's infrastructure. Currently there are five other navigation systems under development by the EU, China, Russia, Japan and India, which will add to the complexities, dependence, vulnerabilities and potential conflict.

Despite these levels of dependence and threat, outer space remains dangerously under-regulated. The last significant piece of international legislation determining behavior in outer space came in 1967.

New legislation will need to be made, and new treaties and protocols to settle issues as varied as planet and moon colonization, space mining, orbital traffic rules, accidental crashes and guidance around the use of force etc.

Outer space is a major and consequential "global commons", and the collective responsibility of humankind. If space becomes critically unsafe, it will not be selectively unsafe, but will be unsafe for everyone. Outer space conflicts will be cascading, and mankind will risk the interruption of many of our daily activities that we take for granted, thus potentially setting back humanity's progress for decades.

Zero-sum approaches will not work in space given its global commons nature; what is needed is what I have termed a "multi-sum security paradigm" coupled with a "Symbiotic Realism" framework.

Written by

Nayef Al-Rodhan, Honorary Fellow, St. Antony's College, Oxford University