# 1AC vs Policy (send)

## \*\*\*1AC\*\*\*

### 1AC - Advantage

#### Private Chinese companies are launching satellites --- that’s key to commercial 5G

Chen 1-21 [Stephen Chen investigates major research projects in China, a new power house of scientific and technological innovation. He has worked for the Post since 2006. He is an alumnus of Shantou University, the Hong Kong University of Science and Technology. “China to start building 5G satellite network to challenge Elon Musk’s Starlink.” Jan. 21, 2022. https://www.scmp.com/news/china/science/article/3164140/china-start-building-5g-satellite-network-challenge-elon-musks]

China will start building a network of a thousand satellites to provide 5G coverage within the next three months, according to state media reports. The first batch of six low-cost, high-performance communication satellites have been produced, tested and arrived at an undisclosed launch site, according to a report by the state news agency Xinhua on Tuesday. The company behind the project, Beijing-based start-up GalaxySpace, has said it wants to extend China's 5G coverage around the world and compete with Starlink, owned by Elon Musk's firm SpaceX, in the market for high-speed internet services in remote areas. The Chinese constellation is small compared with Starlink, which already has around 2,000 satellites in orbit and plans to expand this to 42,000 when the network is complete. Despite its smaller size, the 1,000-satellite Chinese network will be the first of its kind to use 5G technology. Scientists involved in the project say this will ensure download speeds of more than 500 megabits per second with a low latency that will be a critical advantage in some demanding applications such as financial trading. Starlink currently offers a download speed of about 110Mbps for civilian use and although it is using a different technology to 5G, it has the potential to offer 6G services in future. Beyond the commercial rivalry, Beijing has identified Starlink, which has signed multimillion dollar contracts with the US military, as a threat to China's national security. In 2020, researchers with the Chinese National University of Defence Technology estimated that it could increase the average global satellite communication bandwidth available to the US military from 5Mbps to 500Mbps. The researchers also warned that existing anti-satellite weapons technology would find it virtually impossible to destroy a constellation the size of Starlink. Zhu Kaiding, a space engineer from the China Academy of Space Technology, which is working with GalaxySpace on the project, said the Chinese project was struggling to keep pace with Starlink, which according to Musk is producing six satellites a day. Zhu did not disclose how quickly China was producing satellites, but in a paper published in domestic journal Aerospace Industry Management in October last year, he said the Starlink programme had forced a satellite assembly line in China to increase its productivity by more than a third. Zhu and colleagues have said that more than half the routine checks carried out at the launch site of high-frequency operations have been cancelled to save time. The new satellites also use many components produced by private companies that have not previously been involved in Chinese space projects - a move that helped reduce the total hardware price of a high-speed internet satellite by more than 80 per cent.

#### Scenario 1 is cyber.

**China’s Huawei is poised to dominate standard-setting.**

**Clark 21**, \*Laurie Clark is a senior reporter at Tech Monitor. Before this, she held reporting positions at NS Tech, Wired UK and IDG. She holds an undergraduate degree in psychology from UCL and a masters in media and journalism from the University of Glasgow; (June 23rd, 2021, “‘Technical standards-setting is shaping up to be the next China-US showdown”, https://techmonitor.ai/technology/technical-standards-setting-shaping-up-next-china-us-showdown)

**In China’s Standards 2035 plan**, unveiled last year, **the country outlined its intentions to dominate the next generation of technologies by taking a pivotal role in setting technical standards**. According to Beijing, “third tier” companies make products; “first tier” companies set standards. **It wants to be a champion** of the latter.

**The plan is seen as intrinsic to China’s ambitions for supremacy in emerging fields such as** AI, quantum, the internet of things, **5G and 6G.** Those ambitions reflect the commonly held belief that we are on the precipice of a fourth industrial revolution, says Richard Ghiasy, senior fellow at the Leiden Asia Centre in The Netherlands. “What we’ve seen in the previous three iterations, is that the nation or **nations that lead that revolution generally tend to lead the world and the world economy**,” he says.

Unsurprisingly, China’s Standards 2035 plan has attracted pushback from the US, which sees it as a threat to Western dominance of global technology markets. President Joe Biden has said the US should become more involved in standards-setting – casting it as a bulwark to China’s growing influence and power. As such, **digital standards-setting is shaping up to be the latest battleground in the geopolitical tussle between the US and China that increasingly focuses on technology.**

“For two and a half centuries, international technology standards have been an engine for wealth creation and dominance largely belonging to the West,” wrote Shawn Kim, head of the Asia Technology research team at Morgan Stanley, in response to the Standards 2035 plan strategy. “However, this is now changing.”

US vs China: the geopolitics of technical standards

Technical standards allow products to work together across different jurisdictions and manufacturers. A prime example is the USB cable, which replaced multiple different types of cords; another is the plug socket, which takes different forms around the world. If each country or company uses its own standards, technologies are not easily interoperable with those made by other countries or companies.

Usually, standards are set by a consortia of industry-leading companies and international industry associations. Standards can emerge from convention, or the market dominance of a particular supplier, or from formal agreements, depending on the industry and product. China missed the opportunity to participate in the standards-setting of the first wave of technologies, including mobile technologies and internet infrastructure. The current industrial revolution is a chance for the nation to remedy that.

**One of the most successful examples of China’s efforts to play a leading role in standards-setting is 5G**. **China’s influence on global 5G standards is mediated through the world-leading status of Huawei**, **China’s national telecoms champion.** **Huawei is more advanced in 5G than its western competitors such as Nokia and Ericsson** or eastern counterparts Samsung and Fujitsu.

**This has made the company an important actor in setting technical standards for 5G**. **Huawei holds the largest number of “standards-essential patents” required to make 5G work**, followed by Nokia and Samsung, according to research provider IPLytics. **The company also leads in standards proposals to the 3rd Generation Partnership Project** (**3GPP**), **an umbrella group** of standards organisations **that develop protocols for mobile telecommunications** – one-quarter of which have been approved.

**Huawei’s indispensability for 5G is reflected in the fact that**, **although the US has successfully pressured allied countries like the UK and Australia to cut the company’s technology** out of their networks, **others** – **including Germany** – **have hesitated to exclude the company entirely**. In another admission of Huawei’s heft, the US allowed American companies to continue working with the company on setting 5G standards after it was placed on a US trade blacklist, for fear that US companies would no longer have a place at the table otherwise.

But 5G isn’t the only technology that Beijing aims to be instrumental in setting, or updating, the standards for. Chinese navigation satellite systems company, BeiDou, is increasingly competing with GPS, which is owned and operated by the US government. It is more accurate in some regions than existing satellite technology, says Ghiasy, and countries such as Pakistan have shifted from GPS to BeiDou. Ghiasy's research has highlighted e-commerce systems, primarily through the influence of Chinese online shopping giant Alibaba, fintech, and smart city technologies, as areas where China is also exerting considerable influence over standards-setting.

**Another ambitious project approach to rewriting international standards came in the form of a Huawei proposal for a new internet protocol**. Huawei claims that it is being developed solely to meet the technical requirements of an increasingly digital world, and has not woven in any particular governance model. But critics have warned it could integrate a system of centralised control into the internet. Countries such as Saudi Arabia, Iran and Russia have reportedly shown an interest in such alternative network technologies.

Influencing the standards-setting process

**One way China promotes its vision for the technical specifications of the future is by increasing its presence at global standards organisations**. **Chinese officials now lead four such bodies**, including the International Telecommunication Union, a specialised agency of the United Nations responsible for information and communication technologies, and the International Electrotechnical Commission, an industry association that publishes international standards for electrical, electronic and related technologies.

Another means of exerting influence is through China’s Digital Silk Road (DSR) project, a subset of the country’s Belt and Road Initiative (BRI). The DSR focuses on setting up digital or technological infrastructure in partner countries. Smart city infrastructure is particularly popular – according to RWR Advisory, Chinese companies have secured 116 deals to install smart city packages globally since 2013, 70 of which are in BRI countries.

Through the DSR, **China can incentivise countries to adopt its technical standards**, **making it too costly and laborious for them to shift to different standards later**. **The initiative combines government powers with industry-leading companies** such as Tencent and Alibaba, says Ghiasy. "It is very much a whole-of-government plus whole-of-private-sector approach, and there are some subsidies and some policy facilitation. It is a more powerful combination, a more effective one at lower rates, than what we generally can offer [to countries] here in the West."

**Both the US and Europe have baulked at China’s recent push to influence global technical standards**. “To some extent, history is repeating itself," says Paul Timmers, research associate at the University of Oxford and former European Commission director for Digital Society, Trust and Cyber Security. "In the '90s, the US was upset that it got bypassed by planned action of European companies in telecoms frequency allocation and realised it had not kept its eye on the ball; today it is both the USA and Europe who painfully realise that to have been naïve or sleeping, while China was moving forward."

Even greater than the geopolitical struggle between the US and China is the battle between two economic models: free-market capitalism and state capitalism. The US hugely benefited from its technological dominance over the past half-century, and the ample investment and political weight that came with that. “However, **the US has funnelled the profits from that huge global advantage into private bank accounts of a small number of people, perhaps at the expense of reinvesting in next-generation technology**,” says Madeline Carr, professor of global politics and cybersecurity at UCL. “And **that is most clearly evident in the reality now that the US has no viable player in the 5G market.”**

Writing in the South China Morning Post, Morgan Stanley's Kim observes that China's current approach is not a historical aberration. “Most nations that drove industrialisation did so via capital and government support... Industrialisation in Germany and Japan was top-down driven, and the US semiconductor industry was formed by state funding for military and space projects.”

**The US appears keen to redress the recent lack of federal tech investment** with a massive chunk of funding poised to be signed off under the US Innovation and Competition Act. But **sceptics aren’t certain this will be enough to make up ground in key technological areas where China is set to accelerate ahead.**

#### The “Huawei model” is exported to allow a Chinese foothold in US infrastructure development and cyber conflict via built in “kill switches”

Morris 20, David Morris, 2/24/2020, David Morris is Vice President of the United Nations Sustainable Business Network for Asia Pacific, which advises the United Nations Economic and Social Commission for Asia and the Pacific. He chaired the UN Asia Pacific Business Forum in 2019, which was held for the first time in Papua New Guinea, and will co-chair the forthcoming Asia Pacific Business Forum. David served as an Australian diplomat for a decade. He analysed security challenges from South East Asia to the Balkans and was a major contributor to highly-respected reform proposals for the United Nations and peacekeeping. He developed new soft power strategies to support Australian business and cultural promotion around the world. “The Huawei Paradox: cyber-risks in a deteriorating geopolitical climate”, David Morris Project, https://www.davidmorrisprojects.com/post/the-huawei-paradox-cyber-risks-in-a-deteriorating-geopolitical-climate

The central security concern rests upon a theoretical proposition that Chinese technology underpinning international communications systems could be weaponised by the Chinese state. The US and its allies, amongst others, distrust the authoritarian Chinese party state and fear its growing technological and military capabilities. Despite being a private firm, observers note Huawei could be co-opted to serve the national security objectives of the Chinese government and forced to facilitate espionage or cyber-attacks (Gilding, 2020). Article 7 of China’s National Intelligence Law of 2017 is particularly cited, which requires that Chinese firms and their employees cooperate with national intelligence agencies lawfully carrying out their work (Girard, 2019). The US government has equivalent powers (Eisenstein & Halpert, 2018).

The risk of espionage would appear on the face of it to be realistic. After all, it is well documented, including in the Snowden and WikiLeaks revelations, that the US and its Five Eyes (Australia, Canada, United Kingdom and New Zealand) partners similarly engage in espionage (Snowden, 2019), including co-opting Apple, Facebook, Google and other firms to collect data (Biddle, 2020). There is no reason to believe China is not doing the same, regardless of the geopolitical climate and regardless of standard government denials. The perennial risks of espionage raise highly technical questions about capabilities of detection and protection. These are relevant questions not only in relation to Huawei, but for all telecommunications systems and the complex global supply chains for equipment and software.

The risk of cyber-sabotage is much more dependent on the state of the geopolitical climate. In a state of contest, confrontation and potential conflict, there is a risk that technically undetectable malicious code or “kill switches” are implanted into 5G networks, which could be used for cyber-attacks on critical infrastructure. Such aggressive actions might have been less likely during previous years when the US and China and other countries were cooperatively engaged in building interdependent economies. Indeed, Huawei has been intent on building its international reputation as a trusted provider of state-of-the-art technology and it would appear to be self-defeating to allow itself to be used as a platform for hostility against its customers. In the new era of geopolitical competition however, featuring new flashpoints of confrontation, economic decoupling and more aggressive positioning by both the US and China, the risks become more likely that firms such as Huawei (or indeed firms on the US side) might be co-opted or compromised for more aggressive security operations. This is not a risk specific to the firm, but a risk of hostile state action.

Looking forward, the security of 5G networks will become even more important for the connected technologies of the future. Indeed, risks will not only be generated by major power geopolitical contest but governments will also need to protect against cyber-attack from other states, terrorist organisations or rogue individuals. Whether Huawei can be enlisted as a partner in protecting against such risks, or whether it is a vector of risk, will depend upon normative perspective. Further, countries along the so-called digital silk road that are cooperating with Huawei to build “smart city” infrastructure may see more opportunities than risks, while observers from liberal democracies will be concerned about how such infrastructure might in turn be used for surveillance and social control. Whether China is exporting authoritarianism along its digital silk road rests upon the question of agency. How safe city or other programs are deployed by host governments is, at the end of the day, a matter for them rather than China (Weiss, 2019). After all, US, European and Japanese firms also export facial recognition technology that could be used to target groups or individuals but are not accused of exporting authoritarianism. This underlines the normative bias that runs through most of the narratives about Huawei.

International relations risk

The Huawei case exposes a critical gap in global governance. Inadequate rules, norms, standards and institutions exist to manage risks of globally interconnected technology. The international community is ill-prepared for the implications of the so-called “fourth industrial revolution” of big data, artificial intelligence and an internet of things, composed of connected devices and networks. The digital economy has emerged at a time of unipolarity in the international system and a weakening commitment from the US, as the dominant power, towards multilateralism. In the early stages of the digital economy, US firms such as Facebook and Google wielded significant, largely unregulated power. While the internet evolved with some private sector oversight of certain rules (such as domain names), it had no agreed set of international norms or standards and certainly no international enforcement. In the absence of rules, norms, standards and institutional enforcement, technologies generating risks have developed ahead of technical capabilities to manage those risks. Indeed, technical experts claim the complexity of telecommunications technology renders it impossible to guarantee against malicious code or backdoors in equipment (Lysne, 2018; Chang, 2020). Nevertheless, the risk of malicious action has not prevented the international community from developing – and abiding by – rules, norms, standards and institutions in numerous areas of strategic importance, from food safety to aviation. The lack of discussion about governance options for emerging technologies is therefore remarkable.

Governance of 5G telecommunications has become embroiled in the US-China geopolitical contest, as has governance of the internet. The US has opposed any expansion of the mandate of the International Telecommunications Union (ITU), one of the oldest international organisations, to govern digital communications. Meanwhile China, has developed a clear ambition to be rule-setter and norm maker in internet governance and cyber sovereignty (Schia & Gjesvik, 2017; Wang, 2020), as well as in other transformational technologies such as blockchain and its applications in finance, manufacturing, transport, food safety and public security (Cai, 2019; Stockton, 2020). Across its “digital silk road” partnerships with developing nations, China has promoted uniform standards for 5G rollout (consistent with those set by the ITU), as well as for artificial intelligence and satellite navigation systems (Chan, 2019). China will likely wield influence amongst its technological partners in the rules, norms and standards that will develop over time. China – together with firms such as Huawei - has been actively promoting its cyber governance model at World Internet Conferences, the ITU, the International Standardisation Organisation and the International Electrotechnical Commission and the two United Nations (UN) working groups, the Group of Governmental Experts and the Open-Ended Working Group. China can be expected to have the support of a significant number of developing countries.

While the US has begun to participate more actively in these forums in recent times, a fundamental clash of world views makes it unlikely consensus can be achieved. The Chinese government’s aims in cyber governance include maintenance of social stability and protection from foreign influence, deemed to require control of domestic information that is perceived as a threat to the regime. Consistent with its combination of Confucian cultural roots and Marxist-Leninist political ideology, the Chinese party states rules “by law”, in contrast with the liberal Western notions, “rule of law” and contested power. China’s approach to cyber governance is therefore focused on the state’s ability to control content, which includes network security, while Western approaches are focused on network security and not content. China proposes global standards for data security, while the US is moving to establish its so-called “Clean Network” to set standards amongst a set of “trusted” partners, which appears to ignore the global interconnectedness of supply chains and in particular data, with the emergence of cloud technologies and electronic commerce that rely upon free flow of data. China and the US also take opposing positions on governance of cyber-warfare capabilities, with China supporting (publicly at least) a UN-supervised ban, while the US prefers the status quo in which it can continue to develop its capabilities (McCarthy, 2019).

The Huawei paradox, combined with the politics of fear and blame during the Covid-19 pandemic of 2020, has amplified the different approaches of the US, with its lack of a governance framework for data security and opposition to multilateral solutions, and China, with its Cyber Security Law and support for global cyber governance. It appears the law of the cyber jungle will persist at the global level while, as will be discussed below, the European Union (EU), with its comprehensive Cybersecurity Act, General Data Protection Regulation (GDPR) and Directive on Security of Network and Information Systems (NIS), models at a regional level the most advanced attempt at rules, norms and standards to guide cyber risk management.

Economic cooperation risk

The denial of supply of advanced semiconductor chips to Huawei by the US appears likely to reinforce China’s geopolitical fears of containment and indeed historic memories of dismemberment by outside powers. Consequently, it can be expected to drive China to double down on its strategy for not only self-reliance and alternative sources of supply but indeed dominance in next generation technologies. It may take some years, but China can be expected to develop a semiconductor industry to rival the US in time. While it is impossible to prove a counterfactual, it has been suggested by Kennedy (2020) that a more “principled interdependence” between US and Chinese supply chains rather than decoupling might have sustained US semiconductor leadership, slowed China’s technological advance and offered opportunities for joint work on risk management. Coercion has been chosen over cooperation in what may yet prove to be a turning point in the deteriorating geopolitical contest between the US and China, which was being extended to impact new firms and new industries at the time of writing.

The economic costs of excluding Huawei alone are considerable. A Huawei-commissioned Oxford Economics report (2019) predicted that restricting Huawei from competitive tenders will lead to increased 5G investment costs of between eight percent to 29 percent over a decade and would have a cost to GDP in 2035 from $2.8 billion in Australia to $21.9 billion in the US. For US semiconductor firms, the export controls on sales to Chinese buyers constitute a major risk to their global business strategies. In a survey of exports in the first four months of 2018, Capri (2018) found Qualcomm relied on China for 60 percent of revenue, Micron over 50 percent and Broadcom about 45 percent. A Boston Consulting Group report forecast a full decoupling with China would reduce the US chip sector revenue by 37 percent and lower its market share to 30 percent, while China’s market share would rise from three percent to 31 per cent (Varas & Varadarajan, 2020). Further, as the geopolitical climate worsens, there is a risk that China will retaliate against US or allied firms. The Chinese government has reportedly drawn up plans to target so-called “unreliable entities”, such as Fedex, which it is alleged allowed shipments of weapons to Hong Kong and mainland China and diverted US packages addressed to Huawei (Wu, 2020). Any tit-for-tat economic coercion between China and the US will pose significant economic risks for third parties if it escalates, as expected, to include more expansive export controls, prosecutions of technology theft and restrictions on joint research and development with Chinese partners (Thomas-Noone, 2020).

Farrell & Newman (2019) coined the phrases “weaponised interdependence” for this phenomenon of a state deploying economic coercion to leverage its asymmetrical power over a global network and “chokepoint effect” to deny network access to an adversary. Now that the US has set the precedent in its campaign against Huawei, how else the tactic might be deployed is not yet clear, with fears in China, for example, that the US could target international payments through its SWIFT system (Zhao, 2020). To be sure, once the process is initiated against a firm or a sector, entire supply chains will be disrupted. The consequent evolution of a new global economy that moves away from market-led globalisation towards state-led spheres of geopolitical influence is uncertain at this point but 2020 may yet turn out to be a tipping point towards a much more geopolitically-infused international business environment. Geopolitical risk analysis is likely to receive much more attention in international business literature.

Risk assessment

The assessment of security, international relations and economic cooperation risks for 5G networks must be made in the context of not only contemporary international relations but over the life of such networks. This means planning for scenarios, including worst case scenarios. The theoretical capability for cyber-attack, for example, might not be a serious risk in some scenarios, but might become a threat in worst case scenarios in which the major powers are escalating confrontation or engaged in conflict. Following his Huawei ban, Australian prime minister, Malcolm Turnbull observed “it’s important to remember that the threat is a combination of capability and intent. Capability can take years or decades to develop … but intent can change in a heartbeat” (Bourke, 2019). The Australian government clearly assessed the risk could become a threat, and therefore adopted a strategy of risk avoidance by banning Huawei all together. Based on distrust of the Chinese party state, the logic of this strategy would be to avoid all critical supply dependencies on China, which has indeed become a common rallying call within the US and some of its allies since.

Any qualitative assessment of risks must take into account two key concepts, likelihood and consequence. The type of political risk will depend on whether the factors generating the risk arise at the firm level, the country level or as a result of the geopolitical environment. Huawei as a firm has been assessed to pose security risks because of the nature of the Chinese party state and the risks are therefore China risks, or geopolitical risks, rather than specific to the firm itself. Equally, the international relations risks that are generated by the case appear to be not simply because of Huawei itself but arise from the diverging interests of the US and China, characterised in particular by the lack of global governance rules, norms, standards and institutions, which have been established and maintained in other sectors, as noted above, from aviation to food security. Further, in relation to economic cooperation risks, Huawei again appears to be simply the trigger case for an emerging trend in the new geopolitical contest for the US and China to deploy economic coercion, to reconfigure supply chains and indeed to reshape globalisation according to geopolitical agendas and, consequently, abandoning the neoliberal and internationalist market-led phase of globalisation that characterised previous decades.

Accordingly, the Huawei case can be assessed as a prime example of geopolitical risk and can therefore only be understood in the context of the international relations, security and consequent economic policies of the major powers. Suppliers and partners of Huawei and indeed any strategically important firms from China or the US must therefore plan to manage geopolitical risks in the current environment. There has traditionally been very little cross-fertilisation between business literature on political risk and international relations literature (Fägersten, 2015), yet this discussion demonstrates that risks for governments, firms and communities in the Huawei case are entirely bound up in questions of international relations and will require new approaches to risk management.

**Falling behind means China controls the global 5G Market – that’s used to weaponize information networks – induces Taiwan War and Cyberattacks**

Kania 19 – Elsa B, an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security, research focuses on Chinese military innovation in emerging technologies, PhD student in Harvard University's Department of Government. “Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy”, CNAS, https://www.cnas.org/publications/reports/securing-our-5g-future, 11-07-2019

China’s quest for 5G dominance has played out within a complex technological and geopolitical landscape.108 Indeed, **different countries have their own security concerns and** considerations, but not all share American assessments of the severity of these risks. **Insofar as American policymakers see China as a great power rival and strategic competitor, allowing Chinese companies to play a key role in American critical infrastructure, or that of U.S. allies and partners, presents grave threats that are untenable and unacceptable for the United States, not only espionage but also outright subversion of this critical infrastructure.**109 **Yet Huawei has continued to expand its global presence, and the U.S. government has yet to present a viable and attractive alternative to working with** Huawei. Many countries may have sunk costs and be “locked in” already to this choice based on earlier decisions, which raises concerns about not only security but also fair competition.110 However, it is encouraging to see emerging consensus among like-minded countries about potential principles and shared approaches to 5G security, particularly through the progress of a recent conference on 5G security in Prague.111 The age of 5G will present new risks and novel threats of disruption or exploitation. **5G** involves far more than just new and faster wireless networks; it **will be a vital component of future critical infrastructure.** Consequently, **the cybersecurity of 5G networks could prove uniquely challenging, considering the high levels of complexity and much greater potential for damage in the case of an attack.** Not only the confidentiality of data on 5G networks but also questions of integrity and assurance will become urgent challenges. Whereas most cyberattacks to date have involved only data theft, an attack against future 5G networks could cause massive damage that might threaten public safety and critical industries in future smart cities.112 The often subpar security of IoT devices, of which there are an estimated 20 billion globally and growing, also presents serious reasons for concern. A high proportion of devices on the U.S. market have been made in China by companies with very poor track records on security.113 While vulnerabilities have been and remain a major concern in the telecom industry for 3G and 4G, the stakes will be even higher for securing 5G networks at all stages of their life cycles.114 In some cases, **supply chains could be weaponized deliberately by adversaries that may prefer to “win without fighting.”**115 **The exclusion of high-risk vendors** is an important measure to mitigate risk but **does not constitute a complete solution.** 5G must be designed and implemented with a holistic approach to security in mind from the start. The development of secure networks must entail more than simply excluding high-risk vendors, requiring rigorous, ongoing testing and screening. Indeed, careful scrutiny should be extended to all aspects of the production, construction, and management of these networks, involving screening of the security of all vendors and carriers. If an end-to-end approach to security is effectively implemented, 5G could prove more secure than our existing networks and critical infrastructure, but the consequences of insecurity would be far graver. In public debates on 5G security, the call and search for a “smoking gun” has been problematic. This framing of the issue has often distracted policymakers from thinking about the greater challenge of mitigating vulnerabilities that tend to be pervasive. Bugs can be just as problematic as backdoors. It is inherently challenging to differentiate an accidental vulnerability from one that is deliberately introduced. The primary difference is intent, which cannot be discerned from code alone. It is encouraging that the 3GPP’s SA3 working group is focusing on security, seeking to ensure that such security concerns will shape the development of standards.116 However, industry and government are just starting to grapple with the full range of issues in play. Given the gravity of these security challenges, the apparent centrality of Chinese companies in the global development of 5G has raised intense concerns. There is a very real risk that vulnerabilities in networks, whether the result of poor security practices or deliberate introduction of backdoors, could be weaponized for leverage or coercive purposes, particularly in a crisis or conflict scenario. Considering China’s history of IP theft and cyberespionage, there is also a real risk such networks could be exploited for purposes of espionage.117 As a Chinese company, Huawei also would be subject to a number of legal demands, regulatory requirements, and mechanisms of coercion that are often ambiguous and expansive.118 Regardless of whether Huawei’s leadership may wish to disregard an order from the Chinese government, China lacks an independent judiciary system for company leaders to plead their case against the government, as Apple did in the United States when it fought an FBI order to unlock an iPhone. Huawei’s claims that it would “say no” to the Chinese government are not credible without indications of the company’s actual ability to do so. **Even if** Huawei **is given the full** benefit **of the doubt**, despite its history and apparent involvement with the Chinese military and intelligence organizations, **Huawei’s products and services have been assessed to be highly insecure, with a much greater prevalence of vulnerabilities relative to their primary competitors**.119 Moreover, **there are reasons to question whether knowledge of any bugs in its equipment could be shared more readily with China’s Ministry of State Security (**MSS**). This risk may be heightened given the influence of MSS in China’s** vulnerabilities **database, not to mention Huawei’s** historical **and continued** linkages **to the Chinese People’s Liberation Army, including military intelligence.**120 **For the** U**nited** S**tates, these risks and security concerns are inextricable from today’s geopolitical exigencies, insofar as the U.S.-China** rivalry **encompasses scenarios for which there is a nonzero probability of conflict, including over Taiwan**. Consistently, **Chinese military writings have** highlight**ed the potential for cyberattacks on critical infrastructure as a prelude to outright warfare.**121 **The presence of equipment from high-risk vendors, such as Huawei, even in rural telecoms is concerning, considering that some of these networks are near military bases, which raises risks of espionage or exploitation. 5G security presents a global challenge that will demand creative and cooperative solutions.** Huawei will likely remain a major player in 5G in a number of countries, including some U.S. allies and partners, that believe the benefits of partnering with it outweigh the risks. Although a criteria-based calculation of risk provides compelling arguments for exclusion of such highly risky players, many nations could still continue current collaborations with Huawei in ways that exacerbate global risks to this emergent ecosystem. **Even if the United States were to succeed in fully securing its own 5G networks, U.S. data and entities may remain reliant, including for military and commercial activities, upon overseas digital infrastructure that could prove highly vulnerable.The presence of Huawei’s equipment in the critical infrastructure of U.S. allies and partners, whose support or location as a staging ground the U.S. military might require to fulfill its treaty obligations in the event of a crisis or conflict, also creates new risks, to an extent that could undermine U.S. capabilities for command and control and power projection.** As Dan Coats, had warned during his time as director of national intelligence (DNI), **“U.S. data will increasingly flow across foreign-produced equipment and foreign-controlled networks, raising the risk of foreign access and denial of service.”**122

#### Taiwan war causes extinction and turns every impact – MAD fails.

Kulacki 22 [Gregory; 3/7/22; China Project Manager @ Union of Concerned Scientists, PhD in Political Theory @ University of Maryland; “Could US Nuclear Weapons Prevent an Attack on Taiwan?”; https://allthingsnuclear.org/gkulacki/could-us-nuclear-weapons-prevent-an-attack-on-taiwan/]

Today, Chinese military manuals teach troops they are training to “fight a conventional war under conditions of nuclear deterrence.” More specifically, they are preparing to fight a war to prevent Taiwanese independence even if the United States threatens to use nuclear weapons to try to stop them. If the United States were to use nuclear weapons against the Chinese forces attacking Taiwan, Chinese military planners intend to retaliate, most likely against US military bases in Okinawa and Guam.

Once it starts, no one can reliably predict how far or how fast a nuclear contagion could spread. The worst-case scenario is too horrible to imagine. Within an hour, every major city in China and the United States could be reduced to rubble. Hundreds of millions of people could be killed. The global economy, and the global environment, could collapse.

It is precisely because of this possible outcome that Chinese communist leaders believe they can safely ignore US threats to use nuclear weapons. This is what the peasant revolutionary leader Mao Zedong meant when he called US nuclear weapons a “paper tiger.”

#### Cyberattacks go nuclear, even if it fails

Vladimir Orlov 20, Founder & Director of the PIR Center, President of the Trialogue Club International, Head of the Center for Global Trends and International Organizations at the Diplomatic Academy, Ministry of Foreign Affairs of the Russian Federation, Co-Founder and Academic Supervisor of the International Dual Degree MA Program in Nonproliferation and Global Security Studies, MGIMO University, Professor at MGIMO University, author (or coauthor) of more than a dozen books and monographs and more than three hundred research papers, articles, and essays, publishes his views in Russian and foreign periodicals, “‘No Holds Barred’ and the New Vulnerability: Are We in for a Re-Run of the Cuban Missile Crisis in Cyberspace?,” SSRN Scholarly Paper, ID 3538078, Social Science Research Network, 02/14/2020, papers.ssrn.com, doi:10.2139/ssrn.3538078

Not hundred per cent of the dialogue has been frozen, fortunately. Certain informal, mostly offthe-record, meetings of US and Russian experts on cyber agenda continue taking place, both through Track 2 and Track 1.5. One of the most intellectually stimulating meetings, with frank exchanges, took place in Vienna in December 2018. The report produced after the meeting stressed “the significant risk […] that cyber-attacks could conceivably lead to a military escalation that may further trigger a nuclear weapons exchange, a fact that became more explicit with the adoption of the current Nuclear Posture Review. This issue gets complicated given that third parties may have the capabilities to invoke a cyber conflict between Russia and the United States. Whether a country or a non-state actor, they could put the two countries on the verge of an armed conflict by attacking critical infrastructure of either of them and making it look as if the aggressor were the other one”[22]. However, one should have no illusion: such informal meetings may be fully fruitful only when their reports and policy recommendations are utilized by the governments. And for that, a warmer climate in bilateral relations is a must. So far, we see exactly the opposite: mercury falling to freezing levels. Risk of cyber clashes growing into a chaotic global cyber war has been emphasized by the UN Secretary-General Antonio Guterres in his Agenda for Disarmament: “Malicious acts in cyberspace are contributing to diminishing trust among States… States should implement the recommendations elaborated under the auspices of the General Assembly, which aim at building international confidence and greater responsibility in the use of cyberspace.[23]” However, as the members of the US-Russian Track 1.5 working group on strategic stability recently concluded, “without a constructive dialogue on cyber issues between the United States and Russia, the world would most likely fail to agree on any norms of responsible behavior of states in cyber space”[24]. Do we really have to survive a cyber equivalent of the Cuban Missile Crisis to realize the importance of achieving some kind of agreement on cyber issues, and on the broader agenda of international information security?[25] Or is that kind of talk plain old alarmism? I don’t want to sound a fatalist, but I am even less keen on sounding like an ostrich that’s buried its head in the sand. We cannot ignore the obvious: whether the world’s most powerful actors like it or not, the world is sliding to another major crisis like the one in 1962. The cyber war is already raging. There are no rules of engagement in that war. The uncertainty is high. The spiral of tension is getting out of control. The cyber arms race is gaining momentum. And there are no guarantees that the next crisis will be controllable, or that it will result in a catharsis as far as international information security regulation is concerned. There’s no telling what will happen once the cyber genie is out of the bottle.

#### Actors have the means and motivations to strike critical infrastructure.

Wintch 21, \*Timothy M. Wintch, an active-duty Major in the United States Air Force. He is currently a graduate student at the Oettinger School of Science & Technology Intelligence, National Intelligence University, in Bethesda, Maryland. Mr. Wintch has over 11 years of experience in command-and-control operations as an Air Battle Manager. He holds a Bachelor of Arts in Politics from the University of California, Santa Cruz, and a Master of Arts in Military Studies from American Military University. (April 20th, 2021, “PERSPECTIVE: Cyber and Physical Threats to the U.S. Power Grid and Keeping the Lights on”, https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/)

Among critical infrastructure sectors in the U.S., energy is perhaps the most crucial of the 16 sectors defined by the Department of Homeland Security. This sector is so vital because it provides the energy necessary to run every other critical infrastructure sector. However, the U.S. power grid, the backbone of the energy sector, is built upon an aging skeleton that is becoming increasingly vulnerable every day. Whether from terrorists or nation-states like Russia and China, the power grid is susceptible to not just physical attacks, but also to cyber intrusion as well. However, much of this threat can be mitigated if the U.S. takes the appropriate steps to safeguard the power grid and avoid a potential catastrophe in the future.

Since Sept. 11, 2001, terrorism on U.S. soil has been at the forefront of American consciousness. Critical infrastructure provides an appealing target because of the disproportionally large impact even a small attack can have on the sectors. In particular, the power grid represents a particularly lucrative target, both in terms of the ease of access and the large impact it can make. The National Research Council stated that the U.S. power grid is “vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale.”[1] Additionally, the physical security of transmission and distribution systems is difficult due to the dispersed nature of these key components, which in turn is advantageous to attackers as it reduces the likelihood of their capture.[2] From 2002-2012, approximately 2,500 physical attacks occurred against transmission lines and towers worldwide and approximately 500 attacks against transformer substations.[3] Terrorists have the motivation to attack the U.S. power grid but the very nature of the grid makes it highly vulnerable. The power grid is not only at risk from physical attacks, but also nation-state cyberattacks.

One nation that has shown both the capability and intent to use attacks against critical energy infrastructure is Russia, as demonstrated in their 2015 annexation of Crimea from Ukraine. A Russian cyber threat group known as Sandworm, which used its BlackEnergy malware, attacked Ukrainian computer systems that provide remote control of the Ukraine power grid.[4] This attack, and another in 2016, each left the capital Kiev without power, prompting cyber experts to raise concern about the same malware already existing in NATO and the U.S. power grids.[5] In any conflict between Russia and NATO, not only would similar cyberattacks pose a threat, but so would potential physical attacks severing fuel oil and natural gas lines to Western Europe. Russia has both the capability and intent to attack critical infrastructure, particularly power grids, during future conflicts in their “hybrid warfare” approach.

Another nation that has the capability to attack critical energy infrastructure is China, representing a threat to not just the U.S. energy infrastructure but also that of our allies whose support would be vital in a major conflict. A recent NATO report highlighted this threat from China’s Belt and Road Initiative, stating that “[China’s] foreign direct investment in strategic sectors [such as energy generation and distribution] …raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military.”[6] Like Russia, China has been active with cyber intrusions in U.S. energy infrastructure. The Mission Support Center at Idaho National Laboratory characterized these as attacks as “multiple intrusions into US ICS/SCADA [Industrial Control Systems/Supervisory Control and Data Acquisition] and smart grid tools [that] may be aimed more at intellectual property theft and gathering intelligence to bolster their own infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the [bulk electric system], as well.”[7] China, therefore, has both the capability and intent to conduct cyber intrusions and attacks for myriad reasons.

Another arm of this threat is the reliance the U.S. energy industry has on imports from China, especially transformers. In early 2020, federal officials seized a transformer in the port of Houston that had been imported by the Jiangsu Huapeng Transformer Company before sending it to Sandia National Laboratory in Albuquerque. Sandia is contracted by the U.S. Department of Energy for mitigating national security threats.[8] The Wall Street Journal reported that “Mike Howard, chief executive of the Electric Power Research Institute, a utility-funded technical organization, said that the diversion of a huge, expensive transformer is so unusual – in his experience, unprecedented – that it suggests officials had significant security concerns.”[9] Previously destined for the Washington Area Power Administration’s Ault, Colo., substation, the transformer is believed to have been seized due to “backdoor” exploitable hardware emplaced by the Chinese prior to shipment.[10] Shortly after these events, President Trump issued Executive Order 13920, “Securing the United States Bulk-Power System,” essentially limiting the import of Chinese-built critical energy infrastructure components due to concerns about cybersecurity.[11] Interestingly, Jiangsu Huapeng “boasted that it supported 10 percent of New York City’s electricity load.”[12]

Franklin Kramer, the former Assistant Secretary of Defense for International Security Affairs, testified before a U.S. House of Representatives Energy and Commerce subcommittee during an energy and power hearing in 2011 and said that a “highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes.” He added that “an outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.”[13] Even the inclusion of features such as smart grids to the overall grid structure poses new vulnerabilities through their connectivity. Kramer stated that “such connectivity means that the distribution system could be a key vector for a national security attack on the grid.”[14]

#### Those attacks cause accidental nuclear escalation.

Klare 19, \*Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association; (November 19th, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation”, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation)

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.12 The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.13

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

#### Cyber-compromised NC3 causes nuclear war.

Klare 19, \*Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association; (November 19th, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation”, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation)

The Nuclear-Cyber Connection

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.6

Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.7 Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.8 Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.9

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to ~~paralyze~~ undermine the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”10

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike.

“The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.11 Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

#### Scenario 2 is digital authoritarianism.

#### Standards leadership allows China to export digital authoritarianism.

Drew et al. 21, \*Dr Alexi Drew, Research Associate, The Policy Institute, King’s College London; (May 7th, 2021, “The Critical Geopolitics of Standards Setting”, https://www.transatlantic-dialogue-on-china.rusi.org/article/the-critical-geopolitics-of-standards-setting)

However, this previously ‘western’ domain is challenged by a Chinese bloc of private industry actors with centrally directed, strategic motivations for their efforts who have managed to leverage the flaws of this system for political and economic advantage.  The market-driven self-regulation model of technical standards has proven itself unsustainable given the geopolitical power achievable through the control of these standards. The marketised approach is easily abusable by a technologically developed nation-state with geopolitical intentions firmly in mind.

Obscurity Through Complexity

Technical standards have the immediate appearance of being both apolitical and ethically neutral. This seems to set them apart from the debate over standards of state behaviour in cyber space concerning espionage and actions below the threshold of armed conflict. Yet, technological standards are unequivocally connected to normative practices of international behaviour and ethics. The extremely complex nature of the standards under consideration in bodies such as the International Organization for Standardization, the International Electrotechnical Commission (IEC), the International Telecommunications Union (ITU), and the Third Generation Partnership Project (3GPP) obscures the very tangible real-world impact that the standards they set have. The 3GPP is responsible for standards setting for mobile telecommunications. It covers everything from 5G through to autonomous vehicles and the Internet of Things. These are the bodies defining how the modern world is constructed.

On the one hand they appear quite benign, responsible for such banalities as the use of Universal Serial Bus (USB) connectors versus proprietary standards. This hardly seems a matter of national security importance. But the same process is responsible for what ultimately shape the basic operating parameters of facial recognition technology in closed circuit television systems, the level of centralised state control at the technical foundations of the internet, and the protections of personally identifiable data. These generate profound implications for international policy and ethics.

Internal Competition vs Strategic Direction

Technical standards setting processes have, historically, been dominated by private sector actors who have had both the capacity to develop a particular technology to the point of holding a significant market share, and the ability to use that market share to advocate for the standardisation of the technology in line with their own production. The market led approach has continued to be the prevailing model by which American companies have globalised the technical standards behind US dominated technological innovation. This privatised form of self-regulation for technology companies is only partially influenced by the approach taken within the EU where some licensing of standards are controlled by state or EU led institutions.

In contrast to this approach the Chinese model has involved a high level of state-oriented direction, oversight, and direct engagement on the creation and signing off technical standards. Efforts to harmonise and centralise technical standards domestically have become increasingly internationalised as the CCP takes this centralised, strategic approach to technical standards setting bodies such as the ITU, 3GPP, and IEC. Technical standards have also become an increasingly central component of the Digital Silk Road with the openly expressed goal of increasing uptake of Chinese technical standards in partner countries.

The implications of this clash between a system of technical standardisation that is driven by the market versus one driven by an authoritarian government subsidised model are a direct challenge to the development of free, open, and ethical technology. Standardisation mechanisms have become political, or rather there has been a gradual realisation of the political power to be gained from the control of technical standards. While the PRC might have come to this awareness first, the US and Europe have since had a rude awakening about the missed opportunity. The privatised model of technical standards setting favoured by European and US markets relies upon the dynamics of financial competition to regulate behaviour. This is in stark contrast to the statist Chinese model.

#### Consolidated digital authoritarianism is brittle---each disruption causes escalating cycles of global AI war AND smart city collapse

Katherine Manstead 20, Non-Resident Fellow at the Alliance for Securing Democracy and Senior Adviser for Public Policy at The Australian National University’s National Security College, “Strong Yet Brittle: The Risks of Digital Authoritarianism,” Alliance for Securing Democracy, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/05/Strong-Yet-Brittle-The-Risks-of-Digital-Authoritarianism.pdf

While digital authoritarianism can enhance regime durability and national power, it also introduces deep-seated vulnerabilities, eight of which are considered below. Significantly, digital authoritarians may find themselves in a state of constant contest with other regime types, trapped in cycles of overreach and backlash, and prone to strategic miscalculations that pull them into interstate conflict. The current turn to digital authoritarianism therefore also has broader implications for international peace and stability.

Brittle Legitimacy

Reliance on information control makes authoritarians brittle. Small chinks in their information control armor could have existential consequences, particularly during political or economic crises (i.e. when the regime needs to rely on control for legitimacy because it is not delivering for citizens). The information and ideas most dangerous to authoritarians include:

• the identity of opposition groups and leaders and their levels of support; 17

• technical means for subverting control of communications and surveillance technologies;18

• ideas about values that transcend state sovereignty, such as liberalism and human rights;19

• evidence that the central government is not delivering efficient outcomes;20 and

• ideas that undermine the myths and narratives used to legitimize authoritarian rule or the power of the ruling elite.21

Constant Contest

Since technologies and ideas are dynamic, the battle for information control is a constant struggle. It can never be ‘won.’ Authoritarians are therefore in a perpetual state of information warfare, inside and outside their regime, and feel perpetually insecure. This dynamic may lead authoritarian governments to assess that it is worth engaging in information or cyberattacks to discredit liberal ideas at their foreign source or to shape or disable systems that jeopardize their information control—despite real risks of conflict escalation and global pushback.

Overreach and Backlash

The fundamental importance of information control to authoritarians increases the likelihood of overreach, leading to cycles of backlash and reprisal. Many perceive China’s heavy-handed narrative warfare in Hong Kong and confrontational efforts to control narratives about coronavirus to be strategic missteps. For example, CCP efforts to stifle dissent by punishing online gaming company Blizzard and the National Basketball Association (NBA) arguably aided Hong Kong protester narratives;22 while CCP obfuscation about coronavirus has prompted unprecedented diplomatic rebukes from world leaders.23 Despite rising international awareness and condemnation of China’s sharp power tactics,24 China is accelerating, not muting, these behaviors.25 One explanation for this is that the CCP calculates that the risks of international backlash (and occasional overreach by its officials) are acceptable, compared with the risk of letting domestic information control falter.

Impaired Feedback Mechanisms

Authoritarians embrace technology to increase the legibility of their societies. But legibility requires cooperation from society. It is facilitated by an open information ecosystem, robust civil society, mechanisms of transparency, and protections for political speech.26 Conversely, information control and technology-enabled systems of surveillance and enforcement discourage accurate reporting and punish whistleblowing, while incentivizing officials to conceal failures and exaggerate successes.27 In 2007, Le Keqiang (before he became China’s premier) described China’s national income figures as “man-made” and unreliable, and noted that more objectively verifiable proxies should be preferred to official statistics collected by provinces.28 Without elections, authoritarians can also struggle to understand public sentiment, a problem highlighted by the Chinese government’s mismanagement of massive ongoing protests in Hong Kong. Party leaders wrongly assessed that the protestors’ grievances were primarily economic rather than political and that they did not enjoy broader public support.29 As Zeynep Tufekci has observed, the costs of China’s “authoritarian blindness” have been immense: a solvable issue (demands to withdraw a relatively unimportant extradition treaty) became “a bigger, durable crisis” with ongoing political consequences.30

China’s delayed reaction to coronavirus is a stark example of the authoritarian legibility and feedback problem. Local officials and hospital administrators in Wuhan suppressed information about the outbreak and punished doctor whistleblowers—depriving other provinces and the central government (not to mention international authorities) of vital signals that would have allowed swifter action to control the pandemic.31 Once authorities acknowledged the pandemic, China deployed the full weight of its digital surveillance capabilities. It was able to implement top-down lockdowns quickly; marshal its tech sector to build health apps; force citizens to download these apps; and access vast commercial holdings of personal data to cross-check compliance. However, it lacked critical bottom-up feedback systems that may have obviated the need for such draconian measures in the first place.32 Indeed, controlling for income and population size, authoritarian regimes appear to be more lethal than democracies during epidemics, arguably because of their closed information ecosystems.33

Overreliance on Technological Systems which ‘Fail Hard’

Many authoritarian governments are embracing AI-driven surveillance and control methods—from ‘smart cities’ to digital currencies, e-payment platforms and social apps. However, when AI systems fail, they tend to fail in unpredictable, often catastrophic ways. While citizens in democracies lament slow adoption of digital governance, authoritarians’ speed comes with the risk that authorities roll out unsafe or vulnerable systems.34 Imagine a critical failure of China’s social credit system—whether by accident or sabotage—which affected the integrity of records. The implications for regime stability could be significant.

AI systems do not need to fail to produce problematic results. They draw insights and make predictions based on correlations in vast datasets but are not good at identifying causal mechanisms. This means that AI systems often produce outcomes which humans cannot reverse engineer or routinely evaluate. Like using asbestos to build a city, AI governance systems might produce good results in the short-term, but inconsistencies or oversights in their approaches could lead to cascading failures that humans struggle to identify, let alone rectify.35

Unintended Consequences from High-Tech Modernism

Fixation by central governments on achieving targets or deploying certain technologies creates incentives for local officials to deploy “technology placebos” that do little to address underlying economic and social concerns. For example, many so-called smart city projects in authoritarian societies have failed to meet development and economic goals. They are fraught with issues such as “unclear strategic goals” (e.g. they often optimize for surveillance, not development) and “inadequate implementation.”36 This problem may be particularly pronounced for less-developed authoritarian governments which have been persuaded, for strategic reasons, to buy Chinese-exported digital surveillance tools that are not customized to local circumstances. These cities may also become locked into unstable or insecure technical architectures37 and economic dependence on China.38

Commitments to targets, and ideological fervor about technology, can also distort commercial decisions and raise unrealistic public expectations. Analysis of China’s AI industry, for example, suggests that companies are eschewing investment in basic research and focusing on quick wins in applied research.39 Additionally, China is already behind on meeting a number of its technology targets40—a lag that will likely be exacerbated by the global economic downturn following the coronavirus pandemic, and rising security fears in foreign markets about the security of Chinese technology and IP theft by its companies.

From a strategic perspective, there are risks that authoritarian governments’ fixation on technology-centric strategies will lead them to overestimate what technology can in fact achieve. For example, Chinese military strategists have posited that AI could lift the ‘fog’ of war and eliminate uncertainty and confusion on the battlefield. This is an ahistorical and unlikely prediction that could inspire miscalculation.41 Russian strategists theorize about how psychological operations might subdue adversaries without a shot being fired—an approach that may overestimate what cognitive warfare can achieve, at least without being combined with other elements of national power.42

Challenges to Social Cohesion

The medium- and long-term social consequences of digital authoritarianism are yet untested. Overreliance on surveillance and enforcement systems could attenuate relationships within a society, exacerbating authoritarians’ underlying low trust problems. Since they tend to reduce citizens to data inputs, these systems may deny citizens’ intrinsic desire for dignity and identity—with unexpected results.43 Information control tactics—such as flooding—can repress opposition, but long-term may exacerbate public uncertainty and decrease business confidence and trust in official information, with implications for social cohesion and economic progress.44

Dysfunctional Innovation Ecosystems

Information control and state-led pushes for technology dominance risk hampering innovation. For example, to achieve Xi Jinping’s ‘Made in China 2025’ goals, the CCP is supporting high-tech monopolies, restricting international collaboration, and yoking the state and market together.45 However, monopolies are notoriously inefficient and cross-border collaboration is an important driver of innovation. Further, innovation works best under free market conditions and in open societies.46 Some analysts argue that China’s success in deploying AI applications is an exception to this rule. However, there is a risk that Chinese companies are prioritizing shortterm breakthroughs (e.g. analyzing existing datasets to find new insights) at the expense of long-term investment in basic research.47 While authoritarians may excel at developing and deploying AI applications, conceptual research is arguably the real engine of AI advancement—and something that will continue to thrive in open societies.

Summary and Further Research

All states face risks in the information age, but the extent to which regime type affects the relative likelihood of these risks materializing, and their magnitude, is understudied. For example, much has been written about liberal democracies’ vulnerabilities to propaganda and foreign interference via social media.48 But while information warfare against open societies is more likely, arguably it is a higher magnitude threat for authoritarians, where control of information is core to regime survival. Similarly, analysts often lament that democratic governments have been slow to digitize governance systems and craft forward-looking technology policy.49 But while digital authoritarians might outcompete democracies in the roll-out of advanced technologies, this creates new vulnerabilities and risks. Inappropriate safeguards and accidents may result in cascading failures, while heavily digitized governance systems may be susceptible to foreign attack. Regime type may also affect the relative ability of authoritarians and democracies to mitigate their information age risks. For example, a democracy can build resilience to cyber and information threats through a variety of civil society and market-based interventions. Digital authoritarians must rely on a more limited set of top-down policy tools. Ultimately, a more systematic effort to map the comparative strengths and vulnerabilities of authoritarians and democracies in the information age could help both to better understand the other’s threat perceptions and manage escalation risks. It might also highlight ways in which democracies can hold digital authoritarians’ core interests at risk, in order to deter authoritarian interference in their own digital environments.

#### AI mismanagement ensures extinction

Karina Vold & Daniel R. Harris 21, Vold is a philosopher of cognitive science and artificial intelligence & an assistant professor at the University of Toronto's Institute for the History and Philosophy of Science and Technology; Harris is a retired lawyer and Foreign Service Officer at the US Department of State, “How Does Artificial Intelligence Pose an Existential Risk?,” Oxford Handbook of Digital Ethics, Ed. C. Veliz., pp 1-34

4.1 AI Race Dynamics: Corner-cutting Safety

An AI race between powerful actors could have an adverse effect on AI safety, a subfield aimed at finding technical solutions to building “advanced AI systems that are safe and beneficial” (Dafoe, 2018, 25; Cave & Ó hÉigeartaigh, 2018; Bostrom, 2017; Armstrong et al., 2016; Bostrom, 2014). Dafoe (2018, 43), for example, argues that it is plausible that such a race would provide strong incentives for researchers to trade-off safety in order to increase the chances of gaining a relative advantage over a competitor.21 In Bostrom’s (2017) view, competitive races would disincentivize two options for a frontrunner: (a) slowing down or pausing the development of an AI system and (b) implementing safety-related performance handicapping. Both, he argues, have worrying consequences for AI safety.

(a) Bostrom (2017, 5) considers a case in which a solution to the control problem (C1) is dependent upon the components of an AI system to which it will be applied, such that it is only possible to invent or install a necessary control mechanism after the system has been developed to a significantly high degree. He contends that, in situations like these, it is vital that a team is able to pause further development until the required safety work can be performed (ibid). Yet, if implementing these controls requires a substantial amount of additional time and resources, then in a tight competitive race dynamic, any team that decides to initiate this safety work would likely surrender its lead to a competitor who forgoes doing so (ibid). If competitors don’t reach an agreement on safety standards, then it is possible that a “risk-race to the bottom” could arise, driving each team to take increasing risks by investing minimally in safety (Bostrom, 2014, 247).

(b) Bostrom (2017, 5-6) also considers possible scenarios in which the “mechanisms needed to make an AI safe reduces the AI’s effectiveness”. These include cases in which a safe AI would run at a considerably slower speed than an unsafe one, or those in which implementing a safety mechanism necessitates the curtailing of an AI’s capabilities (ibid). If the AI race were to confer large strategic and economic benefits to frontrunners, then teams would be disincentivized from implementing these sorts of safety mechanisms. The same, however, does not necessarily hold true of less competitive race dynamics; that is, ones in which a competitor has a significant lead over others (ibid). Under these conditions, it is conceivable that there could be enough of a time advantage that frontrunners could unilaterally apply performance handicapping safety measures without relinquishing their lead (ibid).

It is relatively uncontroversial to suggest that reducing investment in AI safety could lead to a host of associated dangers. Improper safety precautions could produce all kinds of unintended harms from misstated objectives or from specification gaming, for example. They could also lead to a higher prevalence of AI system vulnerabilities which are intentionally exploited by malicious actors for destructive ends, as in the case of adversarial examples (see Brundage et al., 2018). But does AI safety corner-cutting reach the threshold of an Xrisk? Certainly not directly, but there are at least some circumstances under which it would do so indirectly. Recall that Chalmers (2010) argues there could be defeaters that obstruct the self-amplifying capabilities of an advanced AI, which could in turn forestall the occurrence of an intelligence explosion. Scenario (a) above made the case that a competitive AI race would disincentivize researchers from investing in developing safety precautions aimed at preventing an intelligence explosion (e.g., motivational defeaters). Thus, in cases in which an AI race is centred on the development of artificial general intelligence, a seed AI with the capacity to self-improve, or even an advanced narrow AI (as per §3.1), a competitive race dynamic could pose an indirect Xrisk insofar as it contributes to a set of conditions that elevate the risk of a control problem occurring (Bostrom, 2014, 246; 2017, 5).

4.2 AI Race Dynamics: Conflict Between AI Competitors

The mere narrative of an AI race could also, under certain conditions, increase the risk of military conflict between competing groups. Cave & Ó hÉigeartaigh (2018) argue that AI race narratives which frame the future trajectory of AI development in terms of technological advantage could “increase the risk of competition in AI causing real conflict (overt or covert)”. The militarized language typical of race dynamics may encourage competitors to view each other “as threats or even enemies” (ibid, 3).22 If a government believes that an adversary is pursuing a strategic advantage in AI that could result in their technological dominance, then this alone could provide a motivating reason to use aggression against the adversary (ibid; Bostrom, 2014). An AI race narrative could thus lead to crisis escalation between states. However, the resulting conflict, should it arise, need not directly involve AI systems. And it's an open question whether said conflict would meet the Xrisk threshold. Under conditions where it does (perhaps nuclear war), the contributions of AI as a technology would at best be indirect.

4.3 Global Disruption: Destabilization of Nuclear Deterrents

Another type of crisis escalation associated with AI is the potential destabilizing impact the technology could have on global strategic stability;23 in particular, its capacity to destabilize nuclear deterrence strategies (Giest & Lohn, 2018; Rickli, 2019; Sauer, 2019; Groll, 2018; Zwetsloot & Dafoe, 2019). In general, deterrence relies both on states possessing secure second-strike capabilities (Zwetsloot & Dafoe, 2019) and, at the same time, on a state's inability to locate, with certainty, an adversary’s nuclear second-strike forces (Rickli, 2019). This could change, however, with advances in AI (ibid). For example, AI-enabled surveillance and reconnaissance systems, unmanned underwater vehicles, and data analysis could allow a state to both closely track and destroy an adversary’s previously hidden nuclear-powered ballistic missile submarines (Zwetsloot & Dafoe, 2019). If their second-strike nuclear capabilities were to become vulnerable to a first strike, then a pre- emptive nuclear strike would, in theory, become a viable strategy under certain scenarios (Giest & Lohn, 2018).

In Zwetsloot & Dafoe’s (2019) view, “the fear that nuclear systems could be insecure would, in turn, create pressures for states— including defensively motivated ones—to pre-emptively escalate during a crisis”. What is perhaps most alarming is that the aforementioned AI systems need not actually exist to have a destabilizing impact on nuclear deterrence (Rickli, 2019; Groll, 2018; Giest & Lohn, 2018). As Rickli (2019, 95) points out, “[b]y its very nature, nuclear deterrence is highly psychological and relies on the perception of the adversary’s capabilities and intentions”. Thus, the “simple misperception of the adversary’s AI capabilities is destabilizing in itself” (ibid). This potential for AI to destabilize nuclear deterrence represents yet another kind of indirect global catastrophic, and perhaps even existential, risk insofar as the destabilization could contribute to nuclear conflict escalation.

5. Weaponization of AI

Much like the more recent set of growing concerns around an AI arms race, there have also been growing concerns around the weaponization of AI. We use “weaponization” to encompass many possible scenarios, from malicious actors or a malicious AI itself, to the use of fully autonomous lethal weapons. And we will discuss each of these possibilities in turn. In §5.1 we discuss malicious actors and in §5.2 we discuss lethal autonomous weapons. We have combined this diverse range of scenarios for two reasons. First, while the previous Xrisk scenarios discussed (CPAX and an AI race) could emerge without malicious intentions from anyone involved (e.g., engineers or governments), the scenarios we discuss here do for the most part assume some kind of malicious intent on the part of some actor. They are what Zwetsloot & Dafoe (2019,) call a misuse risk. Second, the threats we discuss here are not particularly unique to AI, unlike those in previous sections. The control problem, for example, is distinctive of AI as a technology, in the sense that the problem did not exist before we began building intelligent systems. On the other hand, many technologies can be weaponized. In this respect, AI is no different. It is because AI is potentially so powerful that its misuse in a complex and high impact environment, such as warfare, could pose an Xrisk.

5.1 Malicious Actors

In discussing CPAX, we focused on accidental risk scenarios—where no one involved wants to bring about harm, but the mere act of building an advanced AI system creates an Xrisk. But AI could also be deliberately misused. These can include things like exploiting software vulnerabilities, for example, through automated hacking or adversarial examples; generating political discord or misinformation with synthetic media; or initiating physical attacks using drones or automated weapons (see Brundage et al., 2018). For these scenarios to reach the threshold of Xrisk (in terms of ‘scope’), however, a beyond catastrophic amount of damage would have to be done. Perhaps one instructs an AI system to suck up all the oxygen in the air, to launch all the nuclear weapons in a nation’s arsenal, or to invent a deadly airborne biological virus. Or perhaps a lone actor is able to use AI to hack critical infrastructures, including some that manage large-scale projects, such as the satellites that orbit Earth. It does not take much creativity to drum up a scenario in which an AI system, if put in the wrong hands, could pose an Xrisk. But the Xrisk posed by AI in these cases is likely to be indirect—where AI is just one link in the causal chain, perhaps even a distal one. This involvement of malicious actors is one of the more common concerns around the weaponization of AI. Automated systems that have war- fighting capacities or that are in anyway linked to nuclear missile systems could become likely targets of malicious actors aiming to cause widespread harm. This threat is serious, but the theoretical nature of the threat is straightforward relative to those posed in CPAX, for example.

One further novel outcome of AI would be if the system itself malfunctions. Any technology can malfunction, and in the case of an AI system that had control over real-world weapons systems the consequences of a malfunction could be severe (see Robillard, this volume). We’ll discuss this potential scenario a bit more in the next section. A final related possibility here would be for the AI to itself turn malicious. This would be unlike any other technology in the past. But since AI is a kind of intelligent agent, there is this possibility. Cotton- Barratt et al. (2020), for example, describe a hypothetical scenario in which an intelligence explosion produces a powerful AI that wipes out human beings in order to pre-empt any interference with its own objectives. They describe this as a direct Xrisk (by contrast, we described CPAX scenarios as indirect), presumably because they describe the AI as deliberately wiping out humanity. However, if the system has agency in a meaningful sense, such that it is making these kinds of deliberate malicious decisions, then this seems to assume it has something akin to consciousness or strong intentionality. In general we are far from developing anything like artificial consciousness and this is not to say that these scenarios should be dismissed altogether, but many experts agree that there are serious challenges confronting the possibility of AI possessing these cognitive capacities (e.g., Searle, 1980; Koch and Tonini, 2017; Koch, 2019; Dehaene et al., 2017).

5.2 Lethal Autonomous Weapons

One other form of weaponization of AI that is sometimes discussed as a potential source of Xrisk are lethal autonomous weapons systems (LAWS). LAWS include systems that can locate, select, and engage targets without any human intervention (Roff, 2014; Russell, 2015; Robillard, this volume). Much of the debate around the ethics of LAWS has focused on whether their use would violate human dignity (Lim, 2019; Rosert & Sauer, 2019; Sharkey, 2019), whether they could leave critical responsibility gaps in warfare (Sparrow, 2007; Robillard, this volume), or whether they could undermine the principles of just war theory, such as noncombatant immunity (Roff, 2014), for example. These concerns, among others, have led many to call for a ban on their use (FLI ,2017). These concerns are certainly very serious and more near term (as some LAWS already exist) than the speculative scenarios discussed in CPAX. But do LAWS really present an Xrisk? It seems that if they do, they do so indirectly. Consider two possible scenarios.

(a) One concern around LAWS is that they will ease the cost of engaging in war, making it more likely that tensions between rival states rise to military engagement. In this case, LAWS would be used as an instrument to carry out the ends of some malicious actor. This is because, for now, humans continue to play a significant role in directing the behaviour of LAWS, though it is likely that we will see a steady increase in the autonomy of future systems (Brundage et al., 2018). Now, it could be that this kind of warfare leads to Xrisks, but this would require a causal chain that includes political disruption, perhaps failing states, and widespread mass murder. None of these scenarios are impossible, of course, and they present serious risks. But we have tried to focus this chapter on Xrisks that are novel to AI as a technology and, even though we view the risks of LAWS as extremely important, they ultimately present similar kinds of risks as nuclear weapons do. To the extent that LAWS have a destabilizing impact on norms and practices in warfare, for example, we think that scenarios similar to those discussed in §4.3 are possible—LAWS might escalate an ongoing crisis, or moreover, the mere perception that an adversary has LAWS might escalate a crisis.

(b) A second scenario, described by Geoffrey Hinton, is that killer drones, equipped with explosives and deep learning neural net technology, could (somehow) learn to function independently of their human controllers (Robinson, 2016), and the system could then go on a rampage and destroy humanity. The bracketed “somehow” here is a critical piece of the story. Perhaps the control system has been hacked, in which case we are back to the malicious actor scenario described in §5.1. Or perhaps there is a malfunction, of the sort also described in §5.1. In this latter case, the malfunction could manifest in the form of a “hard takeoff” in which the system undergoes rapid recursive self-improvement (unintended by the designers) and then develops goals that are inimical to human interests. In such a case, we would be at the start of an intelligence explosion and would confront the kind of Xrisk already characterized by CPAX (§3). Our only point here is that upon closer examination, it's hard to see how this scenario looks distinct from ones previously discussed. Hence, the weaponization of AI can pose an indirect Xrisk in several different ways. In general, the more control an automated system has over weaponized systems that can cause real-world destruction, the greater risk there is of that system becoming a target for attack by malicious actors or of there being greater harm due to any accidental system malfunction.

6. Conclusion

Humanity is facing an increasing number of existential threats, many of which are of our own creation. Thankfully, there are also an increasing number of scholars, from a wide range of fields, studying the nature of these risks and strategizing how to mitigate them. But the field of Xrisk studies is still relatively young. There are significant debates being had over how to define the concept of Xrisk, how to understand its sources, and what methodologies should be used to assess these risks. When it comes to Xrisks from AI, these debates continue. Early concerns around AI Xrisks focused on the possibility of an intelligence explosion and the subsequent pathway to a scenario in which a powerful superintelligent AI has misaligned objectives from humanity. These concerns have not gone away, but they have evolved over time. This chapter has provided an up- to-date critical survey of these arguments, both old and new, looking at different foreseeable pathways towards AI Xrisk, possible global disruptions resulting from the emergence of an AI race dynamic between nations, and the weaponization of AI. In particular, we have tried to make the structures of each of these concerns more explicit, such that readers can begin to critically engage with them.

#### Megacity collapse ensures extinction

Julian **Cribb 17**, author, journalist, editor and science communicator, principal of Julian Cribb & Associates who provide specialist consultancy in the communication of science, agriculture, food, mining, energy and the environment, “The Urbanite (Homo Urbanus),” Surviving the 21st Century, Springer, 2017, Cham, pp. 147–169. link.springer.com, doi:10.1007/978-3-319-41270-2\_8

By the mid-twenty-first century the world’s cities will be home to approaching eight billion inhabitants and will carpet an area of the planet’s surface the size of China. Several megacities will have 20, 30, and even 40 million people. The largest city on Earth will be Guangzhou-Shenzen, which already has an estimated 120 million citizens crowded into in its greater metropolitan area (Vidal 2010).

By the 2050s these colossal conurbations will absorb 4.5 trillion tonnes of fresh water for domestic, urban and industrial purposes, and consume around 75 billion tonnes of metals, materials and resources every year. Their very existence will depend on the preservation of a precarious balance between the essential resources they need for survival and growth—and the capacity of the Earth to supply them. Furthermore, they will generate equally phenomenal volumes of waste, reaching an alpine 2.2 billion tonnes by 2025 (World Bank)—an average of six million tonnes a day—and probably doubling again by the 2050s, in line with economic demand for material goods and food. In the words of the Global Footprint Network “The global effort for sustainability will be won, or lost, in the world’s cities” (Global Footprint Network 2015).

As we have seen in the case of food (Chap. 7), these giant cities exist on a razor’s edge, at risk of resource crises for which none of them are fully-prepared. They are potential targets for weapons of mass destruction (Chap. 4). They are humicribs for emerging pandemic diseases, breeding grounds for crime and hatcheries for unregulated advances in biotechnology, nanoscience, chemistry and artificial intelligence.

Beyond all this, however, they are also the places where human minds are joining at lightspeed to share knowledge, wisdom and craft solutions to the multiple challenges we face.

For good or ill, in cities is the future of civilisation written. They cradle both our hopes and fears.

Urban Perils

The Brazilian metropolis of Sao Paulo is a harbinger of the challenges which lie ahead for Homo urbanus, Urban Human. In a land which the New York Times once dubbed “the Saudi Arabia of water” because its rivers and lakes held an eighth of all the fresh water on the planet, Brazil’s largest and wealthiest city and its 20 million inhabitants were almost brought to their knees by a one-in-a-hundred-year drought (Romero 2015). It wasn’t simply a drought, however, but rather a complex interplay of factors driven by human overexploitation of the surrounding landscape, pollution of the planetary atmosphere and biosphere, corruption of officialdom, mismanagement and governance failure. In other words, the sort of mess that potentially confronts most of the world’s megacities.

In the case of Sao Paulo, climate change was implicated by scientists in making a bad drought worse. This was compounded by overclearing in the Amazon basin, which is thought to have reduced local hydrological cycling so that less water was respired by forests and less rain then fell locally. This reduced infiltration into the landscape and inflow to river systems which land-clearing had engorged with sediment and nutrients. Rivers running through the city were rendered undrinkable from the industrial pollutants and waste dumped in them. The Sao Paulo water network leaked badly, was subject to corruption, mismanagement and pilfering bordering on pillage. Government plans to build more dams arrived 20 years too late. “Only a deluge can save São Paulo,” Vicente Andreu, the chief of Brazil’s National Water Agency (ANA) told The Economist magazine (The Economist 2014). Depopulation, voluntary or forced, loomed as a stark option, officials admitted. Although the drought eased in 2016, water scarcity remained a shadow over the region’s future.

Sao Paulo is far from alone: many of the world’s great cities face the spectre of thirst. The same El Nino event also struck the great cities of California, leading urban planners—like others all over the world—to turn to desalination of seawater, using electricity and reverse osmosis filtration (Talbot 2014). This kneejerk response to unanticipated water scarcity echoed the Australian experience where, following the ‘Millennium Drought’ desalination plants were producing 460 gigalitres of water a year in four major cities (National Water Commission 2008)—only to be mothballed a few years later when the dry eased. By the early 2010s there were more than 17,000 desalination plants in 150 countries worldwide, churning out more than 80 gigalitres (21 billion US gallons) of water per day, according to the International Desalination Association (Brown 2015). Most of these plants were powered by fossil fuels which supply the immense amount of energy needed to push saline water through a membrane filter and remove the salt. Ironically, by releasing more carbon into the atmosphere, desalination exacerbates global warming and so helps to increase the probability of fiercer and more frequent droughts. It thus defeats its own purpose by reducing natural water supplies. A similar irony applies to the city of Los Angeles which attempted to protect its dwindling water storages from evaporation by covering them with millions of plastic balls (Howard 2015)—thus using petrochemicals in an attempt to solve a problem originally caused by … petrochemicals.

These examples illustrate the ‘wicked’ character of the complex challenges now facing the world’s cities—where poorly-conceived ‘solutions’ may only land the metropolis, and the planet, in deeper trouble that it was before. This is a direct consequence of the pressure of demands from our swollen population outrunning the natural capacity of the Earth to supply them, and short-sighted or corrupt local politics leading to ‘bandaid’ solutions that don’t work or cause more trouble in the long run.

Other forms of increasing urban vulnerability include: storm damage, sea level rise, flooding and fire resulting from climate change or geotectonic forces; governance failure, civic unrest and civil war exemplified in Lebanon, Iraq and Syria over the 2010s; disruption of oil supplies and consequent failure of food supplies; worsening urban health problems due to the rapid spread of pandemic diseases and industrial pollution and still ill-defined but real threats posed by the rise of machine intelligence and nanoscience (Gencer 2013). The issue was highlighted early in the present millennium by UN Secretary General Kofi Annan, who wrote:

Communities will always face natural hazards, but today’s disasters are often generated by, or at least exacerbated by, human activities… At no time in human history have so many people lived in cities clustered around seismically active areas. Destitution and demographic pressure have led more people than ever before to live in flood plains or in areas prone to landslides. Poor land-use planning; environmental management; and a lack of regulatory mechanisms both increase the risk and exacerbate the effects of disasters (Annan 2003).

These factors are a warning sign for the real possibility of megacity collapses within coming decades. With the universal spread of smart phones, the consequences will be vividly displayed in real time on news bulletins and social media. Unlike historic calamities, the whole world will have a virtual ringside seat as future urban nightmares unfold.

#### Thus the plan: The appropriation of outer space for 5G by private entities of the People’s Republic of China is unjust.

#### Ericsson and Nokia fill in for Chinese commercial 5G --- European 5G goes global

Jeans 20 [David Jeans, tech reporter at Forbes. “Huawei’s Rivals Are Already Filling A $27 Billion Hole Left By US Sanctions.” Oct. 9, 2020. https://www.forbes.com/sites/davidjeans/2020/10/09/huawei-rivals-nokia-ericsson-27-billion-us-sanctions/?sh=313a315ade48]

After more US sanctions have all-but-[destroyed] ~~crippled~~ the future of Huawei’s global networks business — and its efforts to become the dominant 5G provider — dollar signs are already materializing for its rivals. At the crux of Huawei’s withdrawal is an annual $27 billion opportunity for its competitors — including Nokia, Ericsson and Samsung — to become the go-to providers of 5G and other telecommunication services to domestic carriers, says Ryan Koontz, an analyst at Rosenblatt Securities. “It’s a massive economic transition,” says Koontz. “It’s relatively urgent for these carriers to make the change.” The multi-billion dollar market opportunity, which hinges on Huawei’s sales figures for the year ended September, will not evaporate overnight, Koontz says, but will likely be absorbed over the next three to four years. Because Huawei’s equipment is largely non-existent in the US, the most recent sanctions primarily affect its Asia, Latin America and European markets. In Europe, telco giants are already moving in. Nokia announced Friday that it had been chosen by Orange and Proximus to help build 5G networks in Belgium after the local carriers were pressured to drop the Chinese firm. The deal is of particular significance given Belgium’s role as the home of European Union's executive and parliament, and NATO. And last week, Nokia signed a deal with BT, the United Kingdom’s largest telco, to phase out Huawei’s equipment there. While the value of the deal wasn’t disclosed, Earl Lum, founder of the research firm EJL Wireless Research, estimates it could be worth close to $4.5 billion. Huawei’s other rivals, including Ericsson, are expected to sign similar country-wide deals in coming months. For Samsung, the timing of Huawei’s woes have coincided with a boon for its balance sheet after reporting Thursday that it expected third quarter profit to jump 58% year-over-year to $10.6 billion.

#### It's causal --- decreasing China’s 5G increases Western market shares

Morris 18 [Ian Morris, news editor, Light Reading. “Ericsson Pivots Toward Profitability.” April 24, 2018. http://www.telcotransformation.com/author.asp?section\_id=389&doc\_id=742517&page\_number=2]

Even so, when adjusted for foreign exchange effects, sales were up in North America, the Middle East, Africa and Latin America as some customers began preparing for the rollout of 5G networks and others made improvements to their 4G systems. On the downside, there was a deterioration of conditions in China, where service providers have largely finished building their 4G networks. On the networks side, overall net sales were down 9.5%, to SEK28.6 billion ($3.4 billion), while the operating margin rose to 13.5%, from 12.8% a year earlier. Profitability growth was driven partly by interest in Ericsson's latest radio platform. Called simply the Ericsson Radio System (ERS), this generates higher margins than earlier systems and today accounts for about 84% of total radio deliveries, up from just 61% of the total this time last year. It can also be "software-upgraded" to support 5G services as and when they are introduced, say Ericsson executives. (See DT Ditches Nokia From Its German Radio Access Network.) While Ericsson's guidance is based on an assumption it will not see any commercial 5G business until after 2020, Ekholm now expects otherwise. "We think there will be revenues ahead of that, actually," he said. "We will see commercial revenues this year and clearly next year." Much of that interest is coming from North America, where the biggest mobile operators are busily engaged in a 5G marketing battle and where authorities have blocked Huawei and ZTE from doing business with the major operators. Indeed, ZTE has now said its very future could be at stake after US authorities this week banned it from buying US-made components for the next seven years. Watchdogs say the Chinese firm issued misleading and false statements after it last year paid a $900 million fine for breaching sanctions on Iran. (See ZTE in Existential Crisis as It Slams 'Unfair' US Ban, Considers 'Judicial Measures'.) Analysts believe the setback for ZTE could be an opportunity for Western equipment companies like Ericsson and Nokia Corp. (NYSE: NOK), but Ekholm was coy when asked if he had already seen a positive impact. "I think it is too early to comment on that and our focus is on having a competitive product in the market," he told analysts. "Many customers are asking questions and that is not so strange, but let's refrain from summarizing that yet." Ericsson continues to guide for a sales decline in the overall market for radio access networks (RAN) of about 2% this year, after witnessing a much sharper fall in 2018, and now expects RAN market sales to increase at a compound annual growth rate of 2% over the 2018-22 period. The possible risk is that an industry shift to more open and virtualized RAN technologies allows telcos to reduce equipment spending and leads to the emergence of new vendors. (See Nokia Seizes Open RAN Initiative as Ericsson Holds Back.)

#### Chinese 5G is a paper tiger, but ambitions need to be thwarted now

Brake and Bruer 20 [Doug Brake directed ITIF’s work on broadband and spectrum policy from 2013 to 2021. He writes extensively and speaks frequently to lawmakers, the news media, and other influential audiences on topics such as next-generation wireless, rural broadband infrastructure, and network neutrality. Brake is a recognized broadband policy expert, having testified numerous times before Congress, state legislatures, and regulatory commissions, as well as having served on the FCC’s Broadband Deployment Advisory Group. His written commentary has appeared in publications such as Democracy Journal, Ripon Forum, Morning Consult, Roll Call, The Hill, and RealClearPolicy, and he has provided analysis on air for broadcast outlets such as Bloomberg, NPR, CNBC, and Al Jazeera. Alexandra Bruer was a policy analyst at ITIF from 2020 to 2021. She previously served on active duty for five years in the U.S. Army. She holds a Master in Public Policy from the Harvard Kennedy School and a Bachelor of Arts in Government and Near Eastern Studies from Cornell University. “The Great 5G Race: Is China Really Beating the United States?” November 30, 2020. https://itif.org/publications/2020/11/30/great-5g-race-china-really-beating-united-states]

The utilization of different spectrum resources or amounts of bandwidth results in varying levels of performance even with equal levels of infrastructure. This is relevant when comparing China, which so far uses exclusively mid-band spectrum for 5G, with the United States, which has made a large push to focus on high-band coverage. High-band 5G offers the highest performance leap over existing networks, at least where it is available. But that being said, let’s try a rough comparison, assuming the similar spectrum assets and using China’s announcement that it anticipates 600,000 5G base stations by the end of 2020.18 Assume three base stations per Chinese cell site—one for each of the major operators—and we get about 200,000 sites. This could be several times lower if we’re talking logical sites, but it is hard to say—let’s keep the estimate conservative and set that issue aside. The population served also plays a big role in the performance of a given network. China’s population is about 1.39 billion. This is about 4.5 times larger than that of the United States, indicating Chinese operators will need roughly 4.5 times as many base stations as their U.S. counterparts to get a similar level of performance for each user (all else being equal). So, those 200,000 sites work out to about 1 site per 7,000 people. In 2019 alone, U.S. operators invested in 5G-ready cell sites and added 46,000 new cell sites—roughly 1 site per 7,134 people.19 To the uninformed, 600,000 base stations might sound alarming, but understanding what those numbers mean, we’re about neck-and-neck. If we assume that the Chinese sites include logical sites, and the spectral efficiency of their base stations is less, then it appears the United States is clearly in the lead. Figure 1: 5G deployment comparison of United States and China20Graphical user interface, application Description automatically generated Slow and steady may win the race. Whereas the United States is pursuing a gradual, economical deployment of 5G, the problems with China’s rushed 5G deployments are already starting to show. One of Huawei’s own executives went so far as to call China’s 5G “fake, dumb and poor,” mostly due to poor integration with the 4G network.21 Another former official warned in a recent speech that China’s 5G push could become a failed investment.22 While China is no doubt investing substantially in the expansion of its 5G network, including by pressuring its state-owned carriers to invest faster than the market demands, Chinese figures must be properly scrutinized when using them to make U.S. policy decisions. CONCLUSION It is important that the advocates, experts, and policymakers in the United States get these comparisons right if U.S. policy is going to be oriented toward winning the race. Even with these numbers possibly being misrepresented and overinflated, China’s 5G ambitions should not be underestimated. The country’s deliberate all-hands-on-deck approach to fast-track these networks demonstrates China’s commitment to gaining an edge with the industries of the future. And federal, state, and local policy should also work to spur the expeditious and widespread deployment of 5G systems by wireless carriers.23 And policymakers and the media should view Chinese operators’ 5G claims with skepticism. Chinese firms count their 5G deployment and subscribers differently than U.S. operators, so these methodologies can be misleading if improperly compared.

### 1AC - Framing

#### The standard is maximizing expected wellbeing. Prefer ---

#### Extinction outweighs.

--- must preserve infinite lives and generations.

--- question of intergenerational equity.

--- existential threats are underestimated: global public good, intergenerational, unprecedented, scope neglect.

GPP 17 (Global Priorities Project, Future of Humanity Institute at the University of Oxford, Ministry for Foreign Affairs of Finland, “Existential Risk: Diplomacy and Governance,” Global Priorities Project, 2017, https://www.fhi.ox.ac.uk/wp-content/uploads/Existential-Risks-2017-01-23.pdf, Accessed 7/22/2017, Kent Denver-jKIM)

* 1. THE ETHICS OF EXISTENTIAL RISK In his book Reasons and Persons, Oxford philosopher Derek Parfit advanced an influential argument about the importance of avoiding extinction: I believe that if we destroy mankind, as we now can, this outcome will be much worse than most people think. Compare three outcomes: (1) Peace. (2) A nuclear war that kills 99% of the world’s existing population. (3) A nuclear war that kills 100%. (2) would be worse than (1), and (3) would be worse than (2). Which is the greater of these two differences? Most people believe that the greater difference is between (1) and (2). I believe that the difference between (2) and (3) is very much greater. ... The Earth will remain habitable for at least another billion years. Civilization began only a few thousand years ago. If we do not destroy mankind, these few thousand years may be only a tiny fraction of the whole of civilized human history. The difference between (2) and (3) may thus be the difference between this tiny fraction and all of the rest of this history. If we compare this possible history to a day, what has occurred so far is only a fraction of a second.65 In this argument, it seems that Parfit is assuming that the survivors of a nuclear war that kills 99% of the population would eventually be able to recover civilisation without long-term effect. As we have seen, this may not be a safe assumption – but for the purposes of this thought experiment, the point stands. What makes existential catastrophes especially bad is that they would “destroy the future,” as another Oxford philosopher, Nick Bostrom, puts it.66 This future could potentially be extremely long and full of flourishing, and would therefore have extremely large value. In standard risk analysis, when working out how to respond to risk, we work out the expected value of risk reduction, by weighing the probability that an action will prevent an adverse event against the severity of the event. Because the value of preventing existential catastrophe is so vast, even a tiny probability of prevention has huge expected value.67 Of course, there is persisting reasonable disagreement about ethics and there are a number of ways one might resist this conclusion.68 Therefore, it would be unjustified to be overconfident in Parfit and Bostrom’s argument. In some areas, government policy does give significant weight to future generations. For example, in assessing the risks of nuclear waste storage, governments have considered timeframes of thousands, hundreds of thousands, and even a million years.69 Justifications for this policy usually appeal to principles of intergenerational equity according to which future generations ought to get as much protection as current generations.70 Similarly, widely accepted norms of sustainable development require development that meets the needs of the current generation without compromising the ability of future generations to meet their own needs.71 However, when it comes to existential risk, it would seem that we fail to live up to principles of intergenerational equity. Existential catastrophe would not only give future generations less than the current generations; it would give them nothing. Indeed, reducing existential risk plausibly has a quite low cost for us in comparison with the huge expected value it has for future generations. In spite of this, relatively little is done to reduce existential risk. Unless we give up on norms of intergenerational equity, they give us a strong case for significantly increasing our efforts to reduce existential risks. 1.3. WHY EXISTENTIAL RISKS MAY BE SYSTEMATICALLY UNDERINVESTED IN, AND THE ROLE OF THE INTERNATIONAL COMMUNITY In spite of the importance of existential risk reduction, it probably receives less attention than is warranted. As a result, concerted international cooperation is required if we are to receive adequate protection from existential risks. 1.3.1. Why existential risks are likely to be underinvested in There are several reasons why existential risk reduction is likely to be underinvested in. Firstly, it is a global public good. Economic theory predicts that such goods tend to be underprovided. The benefits of existential risk reduction are widely and indivisibly dispersed around the globe from the countries responsible for taking action. Consequently, a country which reduces existential risk gains only a small portion of the benefits but bears the full brunt of the costs. Countries thus have strong incentives to free ride, receiving the benefits of risk reduction without contributing. As a result, too few do what is in the common interest. Secondly, as already suggested above, existential risk reduction is an intergenerational public good: most of the benefits are enjoyed by future generations who have no say in the political process. For these goods, the problem is temporal free riding: the current generation enjoys the benefits of inaction while future generations bear the costs. Thirdly, many existential risks, such as machine superintelligence, engineered pandemics, and solar geoengineering, pose an unprecedented and uncertain future threat. Consequently, it is hard to develop a satisfactory governance regime for them: there are few existing governance instruments which can be applied to these risks, and it is unclear what shape new instruments should take. In this way, our position with regard to these emerging risks is comparable to the one we faced when nuclear weapons first became available. Cognitive biases also lead people to underestimate existential risks. Since there have not been any catastrophes of this magnitude, these risks are not salient to politicians and the public.72 This is an example of the misapplication of the availability heuristic, a mental shortcut which assumes that something is important only if it can be readily recalled. Another cognitive bias affecting perceptions of existential risk is scope neglect. In a seminal 1992 study, three groups were asked how much they would be willing to pay to save 2,000, 20,000 or 200,000 birds from drowning in uncovered oil ponds. The groups answered $80, $78, and $88, respectively.73 In this case, the size of the benefits had little effect on the scale of the preferred response. People become numbed to the effect of saving lives when the numbers get too large. 74 Scope neglect is a particularly acute problem for existential risk because the numbers at stake are so large. Due to scope neglect, decision-makers are prone to treat existential risks in a similar way to problems which are less severe by many orders of magnitude. A wide range of other cognitive biases are likely to affect the evaluation of existential risks.75

#### The introspective connection between pain and pleasure and phenomenal conceptions of intrinsic value and disvalue is irrefutable – everything else regresses – robust neuroscience proves.

Blum et al. 18 Kenneth Blum, 1Department of Psychiatry, Boonshoft School of Medicine, Dayton VA Medical Center, Wright State University, Dayton, OH, USA 2Department of Psychiatry, McKnight Brain Institute, University of Florida College of Medicine, Gainesville, FL, USA 3Department of Psychiatry and Behavioral Sciences, Keck Medicine University of Southern California, Los Angeles, CA, USA 4Division of Applied Clinical Research & Education, Dominion Diagnostics, LLC, North Kingstown, RI, USA 5Department of Precision Medicine, Geneus Health LLC, San Antonio, TX, USA 6Department of Addiction Research & Therapy, Nupathways Inc., Innsbrook, MO, USA 7Department of Clinical Neurology, Path Foundation, New York, NY, USA 8Division of Neuroscience-Based Addiction Therapy, The Shores Treatment & Recovery Center, Port Saint Lucie, FL, USA 9Institute of Psychology, Eötvös Loránd University, Budapest, Hungary 10Division of Addiction Research, Dominion Diagnostics, LLC. North Kingston, RI, USA 11Victory Nutrition International, Lederach, PA., USA 12National Human Genome Center at Howard University, Washington, DC., USA, Marjorie Gondré-Lewis, 12National Human Genome Center at Howard University, Washington, DC., USA 13Departments of Anatomy and Psychiatry, Howard University College of Medicine, Washington, DC US, Bruce Steinberg, 4Division of Applied Clinical Research & Education, Dominion Diagnostics, LLC, North Kingstown, RI, USA, Igor Elman, 15Department Psychiatry, Cooper University School of Medicine, Camden, NJ, USA, David Baron, 3Department of Psychiatry and Behavioral Sciences, Keck Medicine University of Southern California, Los Angeles, CA, USA, Edward J Modestino, 14Department of Psychology, Curry College, Milton, MA, USA, Rajendra D Badgaiyan, 15Department Psychiatry, Cooper University School of Medicine, Camden, NJ, USA, Mark S Gold 16Department of Psychiatry, Washington University, St. Louis, MO, USA, “Our evolved unique pleasure circuit makes humans different from apes: Reconsideration of data derived from animal studies”, U.S. Department of Veterans Affairs, 28 February 2018, accessed: 19 August 2020, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6446569/>, R.S.

**Pleasure** is not only one of the three primary reward functions but it also **defines reward.** As homeostasis explains the functions of only a limited number of rewards, the principal reason why particular stimuli, objects, events, situations, and activities are rewarding may be due to pleasure. This applies first of all to sex and to the primary homeostatic rewards of food and liquid and extends to money, taste, beauty, social encounters and nonmaterial, internally set, and intrinsic rewards. Pleasure, as the primary effect of rewards, drives the prime reward functions of learning, approach behavior, and decision making and provides the **basis for hedonic theories** of reward function. We are attracted by most rewards and exert intense efforts to obtain them, just because they are enjoyable [10].

Pleasure is a passive reaction that derives from the experience or prediction of reward and may lead to a long-lasting state of happiness. The word happiness is difficult to define. In fact, just obtaining physical pleasure may not be enough. One key to happiness involves a network of good friends. However, it is not obvious how the higher forms of satisfaction and pleasure are related to an ice cream cone, or to your team winning a sporting event. Recent multidisciplinary research, using both humans and detailed invasive brain analysis of animals has discovered some critical ways that the brain processes pleasure [14].

Pleasure as a hallmark of reward is sufficient for defining a reward, but it may not be necessary. A reward may generate positive learning and approach behavior simply because it contains substances that are essential for body function. When we are hungry, we may eat bad and unpleasant meals. A monkey who receives hundreds of small drops of water every morning in the laboratory is unlikely to feel a rush of pleasure every time it gets the 0.1 ml. Nevertheless, with these precautions in mind, we may define any stimulus, object, event, activity, or situation that has the potential to produce pleasure as a reward. In the context of reward deficiency or for disorders of addiction, homeostasis pursues pharmacological treatments: drugs to treat drug addiction, obesity, and other compulsive behaviors. The theory of allostasis suggests broader approaches - such as re-expanding the range of possible pleasures and providing opportunities to expend effort in their pursuit. [15]. It is noteworthy, the first animal studies eliciting approach behavior by electrical brain stimulation interpreted their findings as a discovery of the brain’s pleasure centers [16] which were later partly associated with midbrain dopamine neurons [17–19] despite the notorious difficulties of identifying emotions in animals.

Evolutionary theories of pleasure: The love connection BO:D

Charles Darwin and other biological scientists that have examined the biological evolution and its basic principles found various mechanisms that steer behavior and biological development. Besides their theory on natural selection, it was particularly the sexual selection process that gained significance in the latter context over the last century, especially when it comes to the question of what makes us “what we are,” i.e., human. However, the capacity to sexually select and evolve is not at all a human accomplishment alone or a sign of our uniqueness; yet, we humans, as it seems, are ingenious in fooling ourselves and others–when we are in love or desperately search for it.

It is well established that modern biological theory conjectures that **organisms are** the **result of evolutionary competition.** In fact, Richard Dawkins stresses gene survival and propagation as the basic mechanism of life [20]. Only genes that lead to the fittest phenotype will make it. It is noteworthy that the phenotype is selected based on behavior that maximizes gene propagation. To do so, the phenotype must survive and generate offspring, and be better at it than its competitors. Thus, the ultimate, distal function of rewards is to increase evolutionary fitness by ensuring the survival of the organism and reproduction. It is agreed that learning, approach, economic decisions, and positive emotions are the proximal functions through which phenotypes obtain other necessary nutrients for survival, mating, and care for offspring.

Behavioral reward functions have evolved to help individuals to survive and propagate their genes. Apparently, people need to live well and long enough to reproduce. Most would agree that homo-sapiens do so by ingesting the substances that make their bodies function properly. For this reason, foods and drinks are rewards. Additional rewards, including those used for economic exchanges, ensure sufficient palatable food and drink supply. Mating and gene propagation is supported by powerful sexual attraction. Additional properties, like body form, augment the chance to mate and nourish and defend offspring and are therefore also rewards. Care for offspring until they can reproduce themselves helps gene propagation and is rewarding; otherwise, many believe mating is useless. According to David E Comings, as any small edge will ultimately result in evolutionary advantage [21], additional reward mechanisms like novelty seeking and exploration widen the spectrum of available rewards and thus enhance the chance for survival, reproduction, and ultimate gene propagation. These functions may help us to obtain the benefits of distant rewards that are determined by our own interests and not immediately available in the environment. Thus the distal reward function in gene propagation and evolutionary fitness defines the proximal reward functions that we see in everyday behavior. That is why foods, drinks, mates, and offspring are rewarding.

There have been theories linking pleasure as a required component of health benefits salutogenesis, (salugenesis). In essence, under these terms, pleasure is described as a state or feeling of happiness and satisfaction resulting from an experience that one enjoys. Regarding pleasure, it is a double-edged sword, on the one hand, it promotes positive feelings (like mindfulness) and even better cognition, possibly through the release of dopamine [22]. But on the other hand, pleasure simultaneously encourages addiction and other negative behaviors, i.e., motivational toxicity. It is a complex neurobiological phenomenon, relying on reward circuitry or limbic activity. It is important to realize that through the “Brain Reward Cascade” (BRC) endorphin and endogenous morphinergic mechanisms may play a role [23]. While natural rewards are essential for survival and appetitive motivation leading to beneficial biological behaviors like eating, sex, and reproduction, crucial social interactions seem to further facilitate the positive effects exerted by pleasurable experiences. Indeed, experimentation with addictive drugs is capable of directly acting on reward pathways and causing deterioration of these systems promoting hypodopaminergia [24]. Most would agree that pleasurable activities can stimulate personal growth and may help to induce healthy behavioral changes, including stress management [25]. The work of Esch and Stefano [26] concerning the link between compassion and love implicate the brain reward system, and pleasure induction suggests that social contact in general, i.e., love, attachment, and compassion, can be highly effective in stress reduction, survival, and overall health.

Understanding the role of neurotransmission and pleasurable states both positive and negative have been adequately studied over many decades [26–37], but comparative anatomical and neurobiological function between animals and homo sapiens appear to be required and seem to be in an infancy stage.

Finding happiness is different between apes and humans

As stated earlier in this expert opinion one key to happiness involves a network of good friends [38]. However, it is not entirely clear exactly how the higher forms of satisfaction and pleasure are related to a sugar rush, winning a sports event or even sky diving, all of which augment dopamine release at the reward brain site. Recent multidisciplinary research, using both humans and detailed invasive brain analysis of animals has discovered some critical ways that the brain processes pleasure.

Remarkably, there are pathways for ordinary liking and pleasure, which are limited in scope as described above in this commentary. However, there are **many brain regions**, often termed hot and cold spots, that significantly **modulate** (increase or decrease) our **pleasure or** even produce **the opposite** of pleasure— that is disgust and fear [39]. One specific region of the nucleus accumbens is organized like a computer keyboard, with particular stimulus triggers in rows— producing an increase and decrease of pleasure and disgust. Moreover, the cortex has unique roles in the cognitive evaluation of our feelings of pleasure [40]. Importantly, the interplay of these multiple triggers and the higher brain centers in the prefrontal cortex are very intricate and are just being uncovered.

Desire and reward centers

It is surprising that many different sources of pleasure activate the same circuits between the mesocorticolimbic regions (Figure 1). Reward and desire are two aspects pleasure induction and have a very widespread, large circuit. Some part of this circuit distinguishes between desire and dread. The so-called pleasure circuitry called “REWARD” involves a well-known dopamine pathway in the mesolimbic system that can influence both pleasure and motivation.

In simplest terms, the well-established mesolimbic system is a dopamine circuit for reward. It starts in the ventral tegmental area (VTA) of the midbrain and travels to the nucleus accumbens (Figure 2). It is the cornerstone target to all addictions. The VTA is encompassed with neurons using glutamate, GABA, and dopamine. The nucleus accumbens (NAc) is located within the ventral striatum and is divided into two sub-regions—the motor and limbic regions associated with its core and shell, respectively. The NAc has spiny neurons that receive dopamine from the VTA and glutamate (a dopamine driver) from the hippocampus, amygdala and medial prefrontal cortex. Subsequently, the NAc projects GABA signals to an area termed the ventral pallidum (VP). The region is a relay station in the limbic loop of the basal ganglia, critical for motivation, behavior, emotions and the “Feel Good” response. This defined system of the brain is involved in all addictions –substance, and non –substance related. In 1995, our laboratory coined the term “Reward Deficiency Syndrome” (RDS) to describe genetic and epigenetic induced hypodopaminergia in the “Brain Reward Cascade” that contribute to addiction and compulsive behaviors [3,6,41].

Furthermore, ordinary “liking” of something, or pure pleasure, is represented by small regions mainly in the limbic system (old reptilian part of the brain). These may be part of larger neural circuits. In Latin, hedus is the term for “sweet”; and in Greek, hodone is the term for “pleasure.” Thus, the word Hedonic is now referring to various subcomponents of pleasure: some associated with purely sensory and others with more complex emotions involving morals, aesthetics, and social interactions. The capacity to have pleasure is part of being healthy and may even extend life, especially if linked to optimism as a dopaminergic response [42].

Psychiatric illness often includes symptoms of an abnormal inability to experience pleasure, referred to as anhedonia. A negative feeling state is called dysphoria, which can consist of many emotions such as pain, depression, anxiety, fear, and disgust. Previously many scientists used animal research to uncover the complex mechanisms of pleasure, liking, motivation and even emotions like panic and fear, as discussed above [43]. However, as a significant amount of related research about the specific brain regions of pleasure/reward circuitry has been derived from invasive studies of animals, these cannot be directly compared with subjective states experienced by humans.

In an attempt to resolve the controversy regarding the causal contributions of mesolimbic dopamine systems to reward, we have previously evaluated the three-main competing explanatory categories: “liking,” “learning,” and “wanting” [3]. That is, dopamine may mediate (a) liking: the hedonic impact of reward, (b) learning: learned predictions about rewarding effects, or (c) wanting: the pursuit of rewards by attributing incentive salience to reward-related stimuli [44]. We have evaluated these hypotheses, especially as they relate to the RDS, and we find that the incentive salience or “wanting” hypothesis of dopaminergic functioning is supported by a majority of the scientific evidence. Various neuroimaging studies have shown that anticipated behaviors such as sex and gaming, delicious foods and drugs of abuse all affect brain regions associated with reward networks, and may not be unidirectional. Drugs of abuse enhance dopamine signaling which sensitizes mesolimbic brain mechanisms that apparently evolved explicitly to attribute incentive salience to various rewards [45].

Addictive substances are voluntarily self-administered, and they enhance (directly or indirectly) dopaminergic synaptic function in the NAc. This activation of the brain reward networks (producing the ecstatic “high” that users seek). Although these circuits were initially thought to encode a set point of hedonic tone, it is now being considered to be far more complicated in function, also encoding attention, reward expectancy, disconfirmation of reward expectancy, and incentive motivation [46]. The argument about addiction as a disease may be confused with a predisposition to substance and nonsubstance rewards relative to the extreme effect of drugs of abuse on brain neurochemistry. The former sets up an individual to be at high risk through both genetic polymorphisms in reward genes as well as harmful epigenetic insult. Some Psychologists, even with all the data, still infer that addiction is not a disease [47]. Elevated stress levels, together with polymorphisms (genetic variations) of various dopaminergic genes and the genes related to other neurotransmitters (and their genetic variants), and may have an additive effect on vulnerability to various addictions [48]. In this regard, Vanyukov, et al. [48] suggested based on review that whereas the gateway hypothesis does not specify mechanistic connections between “stages,” and does not extend to the risks for addictions the concept of common liability to addictions may be more parsimonious. The latter theory is grounded in genetic theory and supported by data identifying common sources of variation in the risk for specific addictions (e.g., RDS). This commonality has identifiable neurobiological substrate and plausible evolutionary explanations.

Over many years the controversy of dopamine involvement in especially “pleasure” has led to confusion concerning separating motivation from actual pleasure (wanting versus liking) [49]. We take the position that animal studies cannot provide real clinical information as described by self-reports in humans. As mentioned earlier and in the abstract, on November 23rd, 2017, evidence for our concerns was discovered [50]

In essence, although nonhuman primate brains are similar to our own, the disparity between other primates and those of human cognitive abilities tells us that surface similarity is not the whole story. Sousa et al. [50] small case found various differentially expressed genes, to associate with pleasure related systems. Furthermore, the dopaminergic interneurons located in the human neocortex were absent from the neocortex of nonhuman African apes. Such differences in neuronal transcriptional programs may underlie a variety of neurodevelopmental disorders.

In simpler terms, the system controls the production of dopamine, a chemical messenger that plays a significant role in pleasure and rewards. The senior author, Dr. Nenad Sestan from Yale, stated: “Humans have evolved a dopamine system that is different than the one in chimpanzees.” This may explain why the behavior of humans is so unique from that of non-human primates, even though our brains are so surprisingly similar, Sestan said: “It might also shed light on why people are vulnerable to mental disorders such as autism (possibly even addiction).” Remarkably, this research finding emerged from an extensive, multicenter collaboration to compare the brains across several species. These researchers examined 247 specimens of neural tissue from six humans, five chimpanzees, and five macaque monkeys. Moreover, these investigators analyzed which genes were turned on or off in 16 regions of the brain. While the differences among species were subtle, **there was** a **remarkable contrast in** the **neocortices**, specifically in an area of the brain that is much more developed in humans than in chimpanzees. In fact, these researchers found that a gene called tyrosine hydroxylase (TH) for the enzyme, responsible for the production of dopamine, was expressed in the neocortex of humans, but not chimpanzees. As discussed earlier, dopamine is best known for its essential role within the brain’s reward system; the very system that responds to everything from sex, to gambling, to food, and to addictive drugs. However, dopamine also assists in regulating emotional responses, memory, and movement. Notably, abnormal dopamine levels have been linked to disorders including Parkinson’s, schizophrenia and spectrum disorders such as autism and addiction or RDS.

Nora Volkow, the director of NIDA, pointed out that one alluring possibility is that the neurotransmitter dopamine plays a substantial role in humans’ ability to pursue various rewards that are perhaps months or even years away in the future. This same idea has been suggested by Dr. Robert Sapolsky, a professor of biology and neurology at Stanford University. Dr. Sapolsky cited evidence that dopamine levels rise dramatically in humans when we anticipate potential rewards that are uncertain and even far off in our futures, such as retirement or even the possible alterlife. This may explain what often motivates people to work for things that have no apparent short-term benefit [51]. In similar work, Volkow and Bale [52] proposed a model in which dopamine can favor NOW processes through phasic signaling in reward circuits or LATER processes through tonic signaling in control circuits. Specifically, they suggest that through its modulation of the orbitofrontal cortex, which processes salience attribution, dopamine also enables shilting from NOW to LATER, while its modulation of the insula, which processes interoceptive information, influences the probability of selecting NOW versus LATER actions based on an individual’s physiological state. This hypothesis further supports the concept that disruptions along these circuits contribute to diverse pathologies, including obesity and addiction or RDS.