Article Type: Original Article

Abstract: The following essay was born out of the authors' participation in the Hamburg (Insecurity) Sessions 2019: Un-Cancelling the Future, and the discussions that took place in the workshop on Future Weapons and Emerging Technologies. The workshop participants critically addressed such problems as the future of defence technologies and their sociotechnical environments, cybersecurity and surveillance proliferation, and the improvised instruments of insurgency. Our task was to weave the ideas and insights of the workshop's participants into a vision of the world in 2040, and use it to motivate an analysis of the technoscientific imaginaries emerging in the present. From the workshop presentations and discussions we identified three key areas of that allowed us to imagine the outlines and interactions of global security and technoscientific practice in 2040: *ecopolitics*: the exploitation of ecological systems for strategic ends; *technonationalism*: the use of advanced technologies to pursue racialised and nationalistic geopolitical agendas; and the *security continuum*: the extension of conflict modes to all aspects of social life and the open-source proliferation of security tools and techniques.

Keywords: emerging technologies, geopolitics, ecopolitics, technopolitics, future war, technological imaginaries

The War for the Future [Title]

Preface: Inventing the Future [Subtitle Level 1]

The following essay was born out of the authors' participation in the Hamburg (Insecurity) Sessions 2019: Un-Cancelling the Future, and the discussions that took place in the workshop on Future Weapons and Emerging Technologies. The workshop participants critically addressed such problems as the future of defence technologies and their sociotechnical environments, cybersecurity and surveillance proliferation, and the improvised instruments of insurgency. But they also grappled with the problems and challenges of imagining the future in an age of acute contingency and epistemic crisis. The participants displayed a keen awareness of the emerging uncertainties of climate catastrophe, the vexing opacity of global technological assemblages, and the ambiguity of geopolitical interactions in an age of information warfare.

Our task was to weave the ideas and insights of the workshop's participants into a vision of the world in 2040, and use it to motivate an analysis of the technoscientific imaginaries emerging in the present. By combining several scenarios and exaggerating their interactions we hoped to take advantage of the inherent uncertainty of the future, using it to tune our imaginations into the clues latent in the present.

Geopolitics & Technics in 2040 [Subtitle Level 1]

From the workshop presentations and discussions we identified three key areas of that allowed us to imagine the outlines and interactions of global security and technoscientific practice in 2040: *ecopolitics*, *technonationalism*, and the *security continuum*. This is a world of stark contrasts, unpredictable circumstances, vexed conflicts and inherent contradictions.
It is our world, only more so.

Ecopolitics [Subtitle Level 2]

The physical environment in which conflict takes places determines the means employed and the ends pursued, and in 2040 environmental constraints are no longer simply factors for strategic consideration but are themselves instruments and objects of geopolitical practice. This is the context for what we call *ecopolitics*: geopolitically significant efforts to use technological measures to control, manage and secure not only natural resources but entire ecological systems. Such strategies act as the conceptual linkages between security governance, technoscientific invention, agriculture, military and defence planning, and the computational surveillance of the environment. While state and capital interests have always vied for control of nature through extractive industries, in 2040 environments and their inhabitants are not only sources of materials for production but are both instruments of power and sources of insecurity. As a result, ecological practices have become fields of interest and operation for military, security, and intelligence services, and their concomitant science and technology industries.

At the planetary level, between 2020 and 2040 temperatures rise sufficiently to melt large ice sheets and disrupt ocean currents and their associated jet streams, with serious implications for seasonal change, weather patterns and tidal boundaries. Elsewhere, droughts, floods and heatwaves are seasonal regularities, while biodiversity loss disrupts planetary ecological

communities. In those places where international conflict over natural resources and food insecurity are at their most intense—such as the expanding deserts of the Sahel and Central Asia, the heat-belts of the Middle East, or the agricultural pseudo-colonies of Southern Europe—ecopolitical strategies are used to justify national security policies. Under such conditions, claims of necessity and national survival are invoked by desperate or emboldened belligerents alike. As a result, contested resources become not only sources of conflict but the very means of warfare, as rivers are diverted, water tables drained, crops sabotaged, lakes poisoned, fields stripped and forests plundered.

In 2040, under the pressures of climate change and political insecurity, there are continuous flows of people, labour and wealth from ecologically disrupted—and mostly post-colonial—areas into wealthy countries and their urban centres. Migrations are fuelled by famines and civil wars, or by desertification and, increasingly, the drowning of low-lying territories by rising sea levels. The great power nations continue to profit from this disruption, even as they employ their vast security apparatuses to contain and control the flow of wealth, people, and political power. However, several countries from the global south have taken advantage of the reorganisation of global systems to assert control over their natural resources—such as Bolivia with its lithium deposits—and are now able to meet superior powers from a position of relative advantage by leveraging the scarcity of high-value resources.

To assert control over the complex interactions between natural ecological systems and human agricultural industries, some countries increasingly blend environmental sciences with national defence and international security. The protection and sustainable exploitation of ecological systems has become a priority for most of the Nordic states, and entire landscapes have acquired constitutional protections in Costa Rica and the member states of the African Green-Alliance. The ongoing saturation of the world with networked devices and computational systems—even as parts of it became increasingly uninhabitable—has resulted in the increased efficacy of environmental data, and the policies applied to secure and surveil the environment have resulted in remote landscapes fully enmeshed with nets of militarized sensors and monitoring systems. In some places this has the effect of reducing illegal resource extraction and an increase in the volume of data used to develop regenerative ecological policies, while in others it facilitates the expansion of invasive surveillance regimes and the normalisation of security politics. However, in many places over-reliance on the technoscientific infrastructures of networked society has

resulted in a number of epistemic and pragmatic crises, in which the requisite knowledge and action for effective governance is increasingly distanced from the real world and from the lives upon which it acts.

Technonationalism [Subtitle Level 2]

Geopolitical competition over planetary resources and the reactionary insecurities that emerge in response to mobile populations have caused many countries to engage in various forms of 'technonationalism', embedding explicitly racialised political agendas into international norms of war and security. Science and technology act as both site and driver of chauvinistic identity politics, biomedical security assemblages, and zero-sum geopolitical competition. Governments with various forms of technonationalist policies and structures—ranging from China to Belarus, or the United Kingdom after Scottish independence—employ the vast capabilities of security and surveillance to enforce strict control over identity and association, access to social and private welfare, and participation in financial and job markets. This has resulted in increased spatial and social mobility for those privileged by such systems, and intense precarity and insecurity for those without. For those who are ~~categorized~~categorised as problematic, undesirable, or who offer resistance —or simply refuse to acquiesce—it has meant intensified discrimination, marginalisation and violent oppression.

At the border zones and transitional spaces of technonationalist states, biometric surveillance technologies work in tandem with autonomous drone-swarms and other ubiquitous and distributed security countermeasures. For such countries practicing bionomic security (biometric + genomic) in response to ongoing pandemics, 'borders' no longer refer only to international lines between states and nations, but to practices of militarised segmentation and ~~compartmentalization~~compartmentalisation within national and transnational territories. For technonationalists, borders are the spatial logic of the nation-state and are imposed on the whole of society. This is why, despite their often low-rates of accuracy and myriad inherent biases, AI-directed facial recognition and other automated surveillance systems are ubiquitous. However, even in countries practising nationalistic governance and isolationist politics, these technological security assemblages are tightly intertwined with transnational computational networks that facilitate the flow of military and security intelligence, demographic surveillance, ecological and environmental data.

As a result of both the isolationist policies and technological control, nations embracing illiberal forms of governance show increased willingness to use violence against their own populations—the completion of the multi-decade Chinese genocide project against the ~~Uighurs~~Uighurs being only the most obvious example. Increased aggression towards resistant groups is due, in part, to states' enhanced ability to control the flow of media coverage and public information, which prevents any popular outcry and inhibits resistance movements from disseminating their own messages and narratives.

The Security Continuum [Subtitle Level 2]

In 2040, political conflicts and security practices takes place at all levels of means, media and materials, while military and defence strategies embrace the very fabric of society and the sociotechnical mechanisms of knowledge, consensus and communication.

At the level of planetary scale defence and nuclear capabilities, AI-controlled guidance systems are now standard features of intercontinental weapons systems. These pseudo-autonomous systems guide the trajectories of long-range hypersonic delivery vehicles, which work in tandem with low-orbit weapons platforms to combine traditional nuclear weapons with systems designed to disrupt global communications networks. This has had the effect of disrupting strategic stability and accelerating a latent arms race, but has conversely resulted in the reduction of global nuclear stockpiles, as old platforms and systems become technologically obsolete.

Conventional and unconventional warfare see regular use of small-scale swarms of electronically hardened drones and "flying IEDs". The latter are particularly favoured by insurrectionary movements and terrorist organisations and proliferate through additive and low-cost engineering technologies, appearing in both criminal and civilian contexts. These autonomous swarms of 'flying Faraday cages' create immense problems both for military forces and civilian populations, encouraging the development of advanced electronic warfare and shielding systems designed to protect individuals, population centres, and military assets from swarm attacks. This is an arms race that continues to evolve.

In addition to the full spectrum of weapons technologies, states with advanced cyber capabilities wage continuous campaigns involving the simultaneous sabotage, disruption and manipulation of both critical infrastructure and public opinion. Such activities have become fully normalised, both as aspects of warfare and armed conflict, as well as means of covertly shaping the broader

international political environment. Conventional warfare and other forms of security operations are now accompanied by equivalently scaled information and influence operations, using intelligence and information warfare methods aiming to co-opt both mass and elite opinion. Media outlets, journalists and the executives of their parent corporations have become priority targets of state and non-state intelligence organisations, and in many cases receive levels of protection previously reserved for the ultra-wealthy or heads of state.

The deep contradiction of ubiquitous information warfare is that while these strategies of manipulation can act as opportunities to explore options in conflicts without resorting to violent escalation, they can easily exacerbate conditions to the extent that they result in the kinetic escalation of those very conflicts. However, due to the universal vulnerability of software systems, and the insecurity of cryptography brought on by the emergence of functional quantum computing, political actors see the control of meaning and messaging beyond mere technical advantages as essential to their strategic arsenal. Additionally, new forms of decentralised financial transaction and low-cost manufacturing shift supply chains towards ever-more complex and fragile forms of coordination and logistics, affording new speciations of sabotage, surveillance and espionage.

At the societal level, total reliance on information-technological infrastructure has resulted in the proliferation and normalisation of cybercrime and offensive cybersecurity in civilian life. This has been accompanied by the degradation of privacy rights in most countries and has produced both widespread distrust of authority as well as a second-order effect of ~~popularizing~~popularising open-source security measures. While the individual empowerment afforded by information and communication technologies has produced an informed and skilled global citizenry, in combination with global insecurity it has resulted in the proliferation of surveillance and disinformation techniques, not only as political tools but as means of crime and leverage in societal relations. The proliferation of parallel shadow-economies and truly anonymous digital currencies afford the possibility of both advanced personal privacy measures as well as the proliferation of markets for the tools of crime and insurgency.

A History of the Future: 2020 - 2040 [Subtitle Level 1]

2020s [Subtitle level 2]

The geopolitical landscape of the 2020s was composed of several networks of political conflict and social insecurity, which emerged as the world began to feel the effects of high temperatures, extreme weather events and rising sea levels. States and people faced continuous international conflicts and humanitarian crises as a result of resource scarcity, global pandemics, and their associated economic destruction. Throughout this period, all forms of political organisation worked to expand networks and levers of influence upon the control and mechanics of global technological platforms. Economic disparity within and among societies increased vulnerability in most places, even as large populations transitioned out of poverty.

Beginning in 2020 and lasting until 2024, several corona-virus pandemics resulted in significant damage and reorganisation of the global economy, pushing wealthy countries towards increased automation and hybrid systems of social-welfare and privatised governance, while disadvantaged countries suffered massive setbacks in terms of education, development and economic independence. The pandemics also accelerated techno-scientific research into biomedical technologies with security applications, such as serological passporting, full bionomic identity databases, and the development of AI surveillance algorithms trained on gait and postural data, to overcome the widespread normalisation of face-covering masks.

At some point between 2028 and 2030, almost every person on the earth became connected in some way to the internet. The subsequent empowerment of the individual (and the communal) brought on by universal information access and decentralised supply and manufacturing brought many changes impacting security issues, in particular the emergence of effective and transnational peace movements combining the network effects of universal connectivity with the communicative skills of educated and politically sophisticated coalitions across post-colonial and settler communities.

However, the risks of universal connectivity were highlighted by the Russian cyberattacks against Georgia during the 2029 border conflict, which became known as the ‘world’s first cyber war’. In the midst of a covert military buildup, Russian cyber operators targeted electrical grids, hospitals, government facilities, university and scientific databases, industrial control systems, and even networks of personal computers. Through a combination of espionage and computer network attacks, disinformation campaigns and indiscriminately destructive malware, IT infrastructure all

across the country was exploited, corrupted and in many cases destroyed. The cyberattack was the first in history known to have resulted in the loss of life, caused untold destruction of value and vital information, and was ultimately the triggering event for a border war that resulted in Russian annexation of Georgian territory.

The other significant geopolitical event of the 2020s was the escalation of the conflict between the coastal states that claim territorial sovereignty in the South China Sea. Competing interests over access to resources, national prestige and geopolitical influence were brought to a head with the introduction of both new technologies and new tactics. First amongst these was the disruption of global trade and supply chains by using autonomous underwater weapons systems to close or deny straits and sea lanes through ~~adaptible~~adaptable and only partially detectable blockades, a tactic developed and perfected by the Chinese military and used to great geopolitical effect. Their ability to use relatively cheap autonomous weapons platforms to disrupt global maritime security gave the Chinese the upper hand in their negotiations with the other claimants to the territorial disputes, and forced the other nations of the world to accede to their demands for territorial recognition, or face a trade and supply crisis.

2030s [Subtitle level 2]

After disruptions of the 20s the shifting configuration of international conflict settled into an uneasy assemblage of traditional alliances and competition, economic and technological entanglement, constant and antagonistic cyber and information warfare, grinding infra-state and transnational civil conflicts, and sporadic great power confrontations; a state of 'hanging on' rather than 'hanging together'.

During this period, the density, intensity and acceleration of planetary-scale computation in many instances reorganised the balance of power and caused dramatic reversals of formerly stable political relationships, such as between labour and capital. The most obvious effect was the emergence of public-private alliances that reconfigured the role of both state and capital institutions in international politics. In several cases, vital governance functions (military, education, medical) were given over to private consortiums in order to avoid state collapse, while in others it was a combination of the private sector's exploitation of weak governments and a logical evolution of neoliberal economic policy. Thus the geopolitical landscape completed the shift from post-Cold War unipolarity to an asymmetric global multipolarity, with hegemony shared

between, negotiated and parcelled out between several great power states and their security alliances (Five Eyes/Fourteen Eyes, Belt and Road Security Community, Balkan Defence Initiative, Nordic-Baltic Defence Alliance), which compete both amongst each other and with emerging associations of states and corporate entities (Central Asian Mining Bloc, Pan-African Resource Corporation, Canadian-Arctic Energy Consortium, South Asian Information Alliance). These latter groupings emerged during the shipping and logistics crises that were a result of the Silk Road resource wars and the logistics conflicts in the Arabian Gulf and the South China Sea. By 2040 they had come to control a political sphere of influence in countries where state governance had failed, and so legitimate authority and regional hegemony is assured through a symbolic state-form, while capital, technological and information power are provided by corporate interests.

The parallel and antidote to this process was the emergence of independent state-like movements that focused on collective social-wellbeing and ecological management. This was most prominent in the Middle East, where disruptions to the previous status quo afforded the emergence of the Kurdish Free State of Rojava, a social-ecologist confederation practicing permaculture and acting as a ~~stabilizing~~stabilising actor for regional security; and in the Central American Ecological Confederation, an alliance of states and regions that have ~~utilized~~utilised smart-agricultural practices, shared data-markets and expansive security cooperation to resist the predations of both ~~Panamerican~~Pan-American narco-organisations and American agricultural conglomerates.

The most recent and still ongoing field of geopolitical transformation was the great power competition that emerged in the rapidly thawing arctic, which, beginning in 2035, became a fiercely contested frontier as both the Northern and Northwest Passages became free of ice for large periods of time, opening up new colonial-military projects for natural resources and international influence. This ongoing conflict has drawn in Nordic countries with territorial claims to the Arctic, such as Norway and Finland, as well as the USA and Russia. 2036 saw skirmishes and border clashes between Nordic and Russian armed forces, involving predominantly special forces and unconventional units, but also artillery and mechanised units. Constant mutual surveillance and attempts at sabotage maintain a heightened sense of crisis, which, in combination with the aggressive rhetoric of the nuclear-armed states and their allies, threatens even greater insecurity. In 2038, in combination with a decades-long arms race, the crisis has resulted in both the USA and Russia deploying orbital, hypersonic weapons, with the added

~~destabilizing~~destabilising variable of targeting and guidance systems partially operated by artificial intelligence. Thus, nuclear warfare once again became a clear and present danger.

The Future Present [Subtitle level 2]

Most of these events and upheavals took place not as clearly defined eruptions of violence but as escalations or deteriorations of complex political, ecological and sociotechnical processes. However, looking back at the history of the world we have created it is obvious that for many of these transformations there were a number of alternative options available to those in positions of power, and that the paths chosen were often those affording expedience, convenience, and relative advantage. This was result of the tendency—particularly in the West—to choose and cultivate strategic and technoscientific imaginaries that prioritise the control of present sources of power and efficacy over more long-term perspectives. For the future we can only hope that the means of science, technology and security will be considered not only in terms of their immediate benefit for strategic calculus, but in their wider implications for the ecological systems and social processes in which they unfold.

The Performative Power of Technological Vision(s) [Subtitle level 1]

The scientific revolutions of the past decades have unquestionably conditioned our present (2020) existence, though their extent, effect and geographical distribution has not always been immediately apparent. What has become clear, however, is that where power is situated in defining our present socio-technological relations, and how it manifests in our futures, is effectively disguised by political narratives that depict these progressions as linear and deterministic. Geopolitical hierarchies tend to materialise in the shape of technological capabilities, affording for some the control from the nano to the global level via means of genetic, ecological and geoengineering, global communication networks, or the destructive power of evermore disruptive weapons systems. As a result, the question of who wins or suffers from these technoscientific advances is often sidelined and naturalised through prevailing modes of assessment. Vulnerabilities such as challenges of representation in, or recognition through, technological design and practice are hidden behind regimes of complexity. This tendency is ubiquitous in modern practices of algorithmic warfare (Wilcox 2017), biometric and border technologies (Csernatoni 2018; Kloppenburg and van der Ploeg 2020) as well as in the medical and life sciences (Mehta et al. 2019).

As a pervasive tool of human practice, technology has and continues to transform the material conditions of modern societies. Concordantly, along with technology "the imagination of power and progress in contemporary social life" also changes (Hurlbut and Tirosh-Samuelson 2016: 117). It is this centrality of technoscience and its strategic construction and interpretation in political discourses that we have sought to outline in this exercise, as these processes are already and will likely remain the sites of international competition and political contestation.

The often criticised incursion of security logics, discourses, actors and practices into social, health, and technological realms thereby risks exacerbating existing inequalities within and among societies but also between contemporary and future generations as well as in human/non-human relationships. We argue that these technoscientific security regimes are and will be a dominating factor for the trajectory of our collective futures. They are realised not only materially but through particular modes of contemporary thinking about problems and their solutions that centre on or are mediated through technology and science - and our understanding of them. Touching as much on matters of war(fare) and national defence as on the design and possibilities of healthcare, communication, mobility, government or the state of our environment and climate, technoscientific security regimes have permeated the borders of war and peace, coproducing evermore unbounded theatres of conflict and an expanded battlespace.[1]

They come to matter in the reconfiguration of security practices, the construction of expertise, understandings of subjectivity and the notion of rights as scholars such Claudia Aradau, Tobias Blanke (2018), Trine Villhumsen Berger, Christian Bueger (2015) and Alexander Mankoo (2018) among others have critiqued. But beyond shaping the modes of the present, these processes of co-production have been intimately connected to 'the future' – what it ought to be and whom it is for. Yet the appeal to understand the future through technoscience remains a common trope that Hannah Arendt already cautioned against more than fifty years ago. Replacing all eschatological and moral notions with particular ideas of technoscientific progress for the future, devoid of history and the realm of experiences, yet preoccupied with the idea of human improvement, such a future was empty, senseless and ultimately impossible (Arendt, 1961).

[1] In The Scientific Way of Warfare, Antoine Bousquet (2009) an illustrative analysis of this entanglement epitomized in modern practices of warfare and hegemonic technoscientific epistemes.

Technoscientific Imaginaries & the Future [Subtitle Level 2]

In 2020, we again observe how advances in science and technology promise the consummation of the historical fantasy of human mastery over nature's inherent unpredictability, particularly with regard to 'emerging technologies'. Trends in innovation thereby raise both new and old questions about how to control technology for international security, the practice of science more generally and its agenda for progress (Edwards, 2019). Strategic visions and technoscientific imagination co-evolve in forms of weapons technology, but also in the regimes and infrastructures of data analytics and surveillance or genetic and ecological engineering approaches. We see the ~~aestheticizing~~aestheticising of artificial intelligence and human-machine teaming that seduces us to believe in the abolition of conflict, climate catastrophe, and disease through technological mastery (c.f. Elbe and Roberts, 2016). A technological awe is again palpable, similar to that seen at the beginnings of the nuclear project uniting scientists at Los Alamos and of the Manhattan project for a brief moment in the belief that nuclear weapons would render war obsolete (Masco, 2017).

Such reflections on past national-strategic projects can offer a lens through which to comprehend the workings of the technological-cultural complex in pursuit of security. At its centre remains a dilemma in which, by the very reality of ever more sophisticated military technologies of destruction, the very purpose of these measures—ie the pursuit of security—is compromised (Masco, 2006).

Today's technologies—like Penrose stairs—project these strategic logics into the future through the ways that we make security knowable and enforceable. For example, the promises of big data, enabled through globally interlinked surveillance regimes, nourish anticipations that just "more data" can act as a panacea to our contemporary political and societal uncertainties. In the process of the "delegation of thought" (Leander and Waever 2019: 4) to machines in the analysis and interpretation of our social world we seemingly adapt the question of (in)security to the technical processes that are developed. This "cult of discreetness" eagerly reduces to an instant what is actually "a process and movement, rhythm and relation" to the detriment of those sitting in-between, "those more subtle connections or resonances whose effects are felt but not discrete are overshadowed by those relations we can chart and measure" (ibid) as Jairus Grove (2019: 62) recently critiques.

The COVID-19 pandemic exemplifies the chimeric nature of these security technologies: the goal of globally managing the virus spurred the regimes of surveillance and data mining developed for counterterrorism to find new applications. These technologies, "sitting deep within our agencies as a ~~tantalizing~~tantalising security tool that may become the best means we have of tracking this new 'invisible enemy'" (Doffman, 2020), are empowered through the 'uncanny rhetoric of 'war' (c.f. Draghi, 2020), which has the effect of postponing much of the necessary scrutiny as to their appropriateness, wider ramifications, and even effectiveness (Mudde, 2020).

Demonstrating their ubiquitous utility, these all-encompassing regimes of monitoring, tracking, and policing are here to stay. Civil-military and dual-use projects thereby play into understandings of a security continuum between internal and external security that accelerate strategic international competition in high-tech Research and Development (R&D). The enemy thereby shifts forms and wanders between the dimensions of the global to the microscopic, from global climate change (Rothe, 2016), to terrorist organisations, viruses (Elbe, 2014) and eventually even single base-pairs of our DNA that are causing hereditary diseases. Each is understood to require a technological solution.

Techno-nationalism [Subtitle Level 2]

Achieving and maintaining national leadership in strategic technologies consequently appears as an unquestionable necessity that transforms geopolitical agendas and the ways knowledge, ideas, materials, and skills circulate. Some see concerning resemblances with the arms races and the weaponisation of science and technology that took place during the Cold War (Fink, 2020; Lodgaard 2019). One clear parallel is that the alignment of strategic and security interests with the promises of high-tech and civil-military projects (Csernatoni, 2018) reduces transparency about the intentions of national investment into these "disruptive" technologies (Edwards, 2019).

The field of (Global) Health again provides for illustration of comprehensive civil-military collaboration and the entanglement of research projects, expertise, grants, and discourses. The U.S. Defense Threat Reduction Agency (DTRA) for instance, led decades-long efforts across public and private sectors (such as the pharmaceutical company Merck & Co., Inc., non-governmental and international organisations) to develop the vaccine Ervebo® against the Ebola Virus Disease (EVD) (Gardner, 2020). The vast knowledge, data, and research infrastructure allowing the development of the EVD vaccine, the eradication of smallpox, as well as treatment to other infectious diseases such as polio are no coincidence

but are a product of the extensive strategic interests of Western military institutions in biological weapons/threats throughout (modern) history (Geissler et al, 1999).

Consequently, the funding of and research into orphan diseases such as Ebola through (Western) state agencies such as the military in and of itself is neither new nor is it only problematic. Given the embeddedness of healthcare in the market economy, state funding into rare diseases even serves a crucial function to keep eradicating or treating non-domestically prevalent diseases on the agenda of resourceful pharmaceutical research (companies). Similarly, the 2014-2015 military operation 'United Assistance' during the humanitarian crisis and Ebola epidemic in West-Africa, foremost in Liberia, allowed the crucial logistic support of the Centre of Disease Control (CDC) as well as the allocation of vast resources towards a public health response (Kamradt-Scott et al. 2015).

The other side of the coin, however, presents itself as an amalgamation of strategic, economic, and ~~defense~~defence research interests that is spurring international mistrust. The U.S. Defense Advanced Research Project Agency (DARPA) and its project "Insect Allies" for instance recently sparked suspicion about its officially stated purpose to enhance agricultural production, when the underlying technology also suits itself as a potent biological weapon (Reeves and Voeneky et al. 2019). Meanwhile, much of the mainstream European and Western critique of the expansion of the security continuum has focused on China's national agenda for military-civil fusion (see for instance Kania 2017). Projected into the near to medium-term future, these trends will have a significant impact on the workings of democratic governance in its attempt to guide technological development according to its political commitments. Democratic states should be wary of becoming complicit in fostering these dangerous and often mutually reinforcing accelerations of geopolitical competition. Critical engagement with (the drivers of) these 'domestic' projects thereby is not to be mistaken as moral relativism, but a call for caution that European and US defence research projects equally can spur international competition, secrecy and mistrust exactly over those projects for which public deliberation would be central yet are put aside over fears to lose the strategic advantage.

As long as technoscientific influences on security regimes are considered to be merely neutral and enabling rather than affording and creating path dependence, the strategic choices of state agencies and powerful non-state actors can hide behind conceptions of (technoscientific)

'emergence'. Cut loose from the incremental steps leading to inventions and the generation of knowledge, these narrations evoke ideas of the inevitability of technology and the linearity (or singularity) of technology-induced progress. Hidden in this technocratic line of reasoning are the ways our terms of reference and debate become trapped in sequences of tokenised frameworks that neglect substantive discussion as to whether any alternative means are available. Andy Stirling (2018) recently critiques:

> the choices for innovation are restricted to the balancing of "risk" and "benefit" in some singular and supposedly inevitable direction for advance. Too often, the issues are reduced simplistically to a spectrum from "forging ahead" to "falling behind", as if the direction were predetermined or self-evident (Stirling, 2018 7-8).

The view of alternative fields of technological production and meaning-making helps us to recognise where power and hierarchy is situated in its construction. An increasing interest in Do-It-Yourself (DIY) and Citizen Science broadens the application of science according to individual or community needs. While DIY science, as well as the notion of the 'democratisation', has regularly been associated with proliferation concerns and terrorism (Clapper, 2016), crowd-funded projects such as 'Open Insulin' (Burningham, 2019) and the growth of open-source information security knowledge, demonstrate efforts to challenge the gatekeeper role of traditional actors. This has impacts upon definition of scientific and technological objectives and their influence in the production and circulation of essential technologies. The outlook of enhanced production of local products thereby adds to the variety of technological options available in the future, allowing customers to choose between options and expand the technoscientific literacy. It corrects those claims for technology's determinist effects on society by acknowledging "not that technology develops outside of human agency, but that it develops outside of some humans' agencies" (McCarthy, 2013: 476). That is, attempting to understand the symbolical and material power of technoscientific projects through their embeddedness in and coproduction through socio-political relations.

Where Do We Go from Here? [Subtitle Level 1]

Thus far we have illustrated a dominant theme of the present that underlies the future we imagined at the opening of this piece: the opaque, competitive and often naive political discourse on technoscientific developments elides the complex political and strategic issues generated by

technological invention. Whereas our outlined future may – or most likely may not – come true, our contribution is to make the future thinkable and thereby consciously changeable.[2]

Meanwhile, large technological projects—such as those of the nuclear age and the emerging fields of genetic design—struggle with their "unthinkability" (Masco, 2006: 3), even as their development and concomitant investment renders them seemingly necessary and inevitable. Their effects, for different reasons, appear too overwhelming and radical to be comprehended within and through the everyday. They appear as the subjects of science fiction or in the form of news reports on scientific 'breakthroughs' that spark awe and wonder rather than a thorough debate about their socio-political embeddedness. Although not a novel phenomenon, such understandings render us unable (or unwilling) to critically steer technological developments at the time of their emergence. Yet the situation is not all doom and gloom: the nuclear age has also demonstrated opportunities to spark discourses about vulnerability and insecurity. These can form starting points for emancipatory agendas that refocus the terms of progress from the centrality of the machine to the quality of everyday life and the fragility of the human body and the virtues of sociopolitical interdependence.

Although the tech-sector is temporarily under the spotlight of public attention and scrutiny within the political debate, it is unclear if and how this might relate to deeper changes in the relationship between innovation and democratic institutions. Part of the problem is the way tat social inquiry into technology is structured, and how 'the problem of technology' is perceived and articulated. As we noted above, technological vision is performative. Yet the predicament we see is also a shortcoming of contemporary political engagement with public administrations dealing with emerging technologies.

Big tech companies such as Amazon, Google/Alphabet, and Facebook have started to acknowledge their significant role in core political processes such as democratic elections and the formation of political opinion (i.e. "The corporate responsibility to protect" (MSC, 2020)). Yet parliamentary inquiries (i.e. UK Parliament Committee on Digital, Culture, Media and Sport (2018)) highlight the lack of robust political-legal foundation that defines these companies' responsibilities towards the public. This is a topic that increasingly figures on the

[2] It thereby deviates from methodological approaches such as Delphi method-informed Horizon Scanning that aim to systematically (and accurately) identify upcoming opportunities or threats from technological, regulatory or socio-political changes (Sackmann, 1975; Sutherland and Woodroof, 2009).

political agenda, and Silicon Valley elites themselves should consider the professionalisation of their political representation, as was suggested during the 2020 Munich Security Conference by a Member of the US Congress.[3] Absent of internal consultation and coordination, both political decision-makers and the tech-sector hinder fruitful exchange of expertise and experience supporting regulation, but also safeguards against misuse or adverse scenarios.

Recent interest in how both innovations and unconscious biases emerge in technological features has contributed to a wider awareness about who participates in the process of technological design, and the many ways that vulnerabilities, exclusion, racism, sexism, etc. materialise in our (technological) institutions. As a result of the critical interrogations of these dynamics we can observe the importance not only of professional expertise but also the value of 'lay' knowledge in considerations of how we might achieve a meaningful 'democratisation' of technology. A thoughtful account of the relationship between expertise, lay knowledge, and the means of participation in the technical sphere has been advocated by scholars in the field of science and technology studies and philosophy of technology. Such enquires have as their premise the idea that agency neither is nor ought to be limited to expert groups, but ought to be, as suggested by Feenberg (2017), available to individuals through their interaction with and experience of technologies and associated systems. The socio-technical relationship he describes is thereby both co-productive and the result of an "entangled hierarchy", in which social groups on the one hand "exist through the technologies that bind their members together", yet through this membership also gain power over technological developments, "through their choices and protests." Controversies surrounding Genetically Modified Organisms (GMO) – and their use in agriculture and farming – especially within societies of EU Member States, have demonstrated that public intervention can alter technological institutions, their codes, practices, and regulations. Undoubtedly, such interventions remain structured by and embedded in pre-existing norms and economic interests, which for instance have formed European sensitivities over the desirability of human intervention into nature (Felt 2015). Nevertheless, they also point to the potency of public deliberation in creating and maintaining these norms to change both the design and application of technological artefacts.

[3] Comment by U.S. Congress Member Elissa Slotkin during a Townhall debate on the Future of Disinformation, Munich Security Conference 15th February 2020.

For security, public participation comes to matter in light of increasing trends of dual-use and civil-military collaboration, for instance, promoted within the European Horizon 2020 framework. Agendas such as 'Responsible Research Innovation' imitative promoted within the same framework could foster both the ethical understanding of those at the forefront of technological innovation as well as public deliberation over the political ends (and means) of dual-use innovation. Controversies over US DoD's Project Maven (ICRC, 2018; Weisgerber, 2018) furthermore uncovered the unease the convergence of private technical expertise and capacity with national strategic interests unleashes, demonstrated with the political mobilisation of Google's tech workers.[4] These events uncovered both essential discrepancies in innovation cultures between the Silicon Valley enterprises and traditional security contractors, but also pointed to the strategies deployed by the US DoD since to unite innovation capabilities in line with the 'national interest'.

On this point, yet coming from a different angle, several governance initiatives exist that seek to break down barriers between sectors, areas of expertise, and skillsets to enable multinational and public-private cooperation. Such initiatives for instance found in the field of disarmament and responsible innovation/science ethics aim to foster collective capabilities across traditional security boundaries in areas such as Life Sciences, Physics and Chemistry that have a long tradition of science-led peace initiatives institutionalised in organisations such as Pugwash. Julian Perry Robinson contended about two decades ago on the rationale of this activism emerging in the aftermath of the use of nuclear weapons:

> Scientists have always had to contend with what has been called their "double loyalty": a sense of duty not only to their country but also to their science. In some disciplines, this duality could be conflictual, and, during those early years of the "national security state", it was indeed for more and more people. Loyalty to science is an abstraction not easily described or understandable outside its world. In some scientists it is nonexistent, but in others, it is passionate, overriding. Maybe it has to do with the desire to protect newborn knowledge from deformation, from distraction, from loss, from waste. Maybe it also has to do with the belief that science is for the common good (Robinson, 1998: 5).

These sentiments since have evoked great progress in terms of ethical sensibilities as well as the creation of strong norms in the conduct of science. In the field of Synthetic Biology and Genome Editing initiatives such as iGEM (International Genetically Engineered Machines competition) have

[4] In a similar vein, employees of Microsoft prominently have held the company to account for its collaboration with the US Immigration and Customs Enforcement to process data and artificial intelligence capabilities (Frenkel 2018).

been established to foster 'good practice' and norm building surrounding principles of responsible research innovation. It successfully incorporates actors from different sectors (i.e. academia, the Do-It-Yourself Community, and security bureaucracies), but also importantly generations to collaborate and exchange on the state-of-the-art in Synthetic Biology but also to generate trust among the different sectors. As a governance model for other emerging technologies, iGEM has successfully integrated adaptive risk management approaches that speak both to the potential social-political problems the life sciences could contribute to while being in dialogue with different stakeholders from early one. For instance, in 2018, iGEM started the collaboration with regulators and experts to develop a risk assessment tool for its teams, whereas it achieves educational goals in requiring teams "to identify and describe the procedures, practices, or containment measures they will use to manage the risks they identify" (Millet et al. 2019).

These initiatives, themselves a model for intersectional collaboration in a fast-changing technological environment are increasingly embedded in conceptual reconsiderations about how regulatory decisions are made beyond normative models of how they ought to. Pragmatist approaches as such of Charles Lindblom (1959, 1979) for instance suggest attending to practices of "muddling through" – acknowledging how decision-makers (need to) align conflicting perspectives and priorities when information is in short supply or contradictory. These conundrums are central to decisions on how and when initial experiments of governance are worth scaling-up. This is of importance for international attempts at achieving greater harmonisation in regulatory landscapes. It is this plural field of actors, skillsets, generations, and geographies that offer the alternative and plural reading frames necessary to 'uncancel' our predetermined technological future and to allow inclusiveness for the visions of those sitting in between the dominant paradigms, and whose visions have too often been neglected and rendered invisible.

Notes on Contributors [Subtitle Level 1]

Samuel Forsythe is a doctoral researcher in International Security at the Peace Research Institute Frankfurt, where he is a member of the Research Group for New Technologies, and a PhD candidate at Goethe University Frankfurt. His thesis examines how geopolitical actors respond to advances in information and communication technology by developing strategic theories and practices that draw upon and reinvent the traditions of cunning, deception and stratagem.

Anna Rößing is a PhD researcher in Conflict and Security at the University of Bath, United Kingdom. Her project investigates the security implications of innovation in advanced biotechnologies. Anna has published in the field of biosecurity and future studies. At the University of Bath, she is part of a new research centre to study the ethical and security dimensions of emerging technologies. Before starting her PhD, she studied Pharmaceutical Sciences at the Ludwig Maximilian University of Munich and gained working experiences in pharmaceutical research and public health. She also holds a MA in Conflict, Security, and Development from the University of Sussex.

References [Subtitle Level 1]

Aradau, C. and Blanke, T., 2018. Governing others: Anomaly and the algorithmic subject of security. European Journal of International Security, 3(1), pp.1-21.

Arendt, H. 1961. Between Past and Future, Eight Exercises in Political Thought, New York Penguin classics.

Austin, Burt, Trivers, R. and Burt, A., 2009. Genes in conflict: the biology of selfish genetic elements. Harvard University Press.

Berling, T.V. and Bueger, C. eds., 2015. Security expertise: Practice, power, responsibility. Routledge.

Burningham, G., 2019. The Price of Insulin Has Soared. These Biohackers Have a Plan to Fix It. Time. Available at: <https://time.com/5709241/open-insulin-project/> [Accessed 27 March 2020].

Clapper, J., 2016. Director of National Intelligence. Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee. February 9, 2016

Doffman, Z., 2020. Coronavirus Reality Check: Yes, U.S. And EU Will Track Our Smartphone Location Data—Get Used To It. Forbes. https://www.forbes.com/sites/zakdoffman/2020/03/19/coronavirus-reality-check-yes-us-and-eu-governments-will-track-our-phones-get-used-to-it/> Accessed 20 March 2020.

Draghi, M. 2020. We face a war against coronavirus and must mobilise accordingly. Retrieved 26 March 2020, from https://www.ft.com/content/c6d2de3a-6ec5-11ea-89df-41bea055720b

Edwards, B. 2019. Insecurity and Emerging Biotechnology: Governing Misuse Potential. Palgrave Macmillan.

Elbe, S. 2014. The pharmaceuticalisation of security: molecular biomedicine, antiviral stockpiles, and global health security. Review of International Studies, 40 (5). pp. 919-938.

European Commission. 2018. Future and Emerging Technologies (FET). Accessed March 01, 2020, from http://ec.europa.eu/programmes/horizon2020/en/h2020-section/future-andemerging-technologies

European Commission. 2018. Future and Emerging Technologies (FET). Work programme 2018–2020. Accessed March 01, 2020, from http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-fet_en.pdf

Esvelt, K. M., Smidler, A. L., Catteruccia, F., & Church, G. M. 2014. Emerging technology: concerning RNA-guided gene drives for the alteration of wild populations. Elife, 3, e03401.

Feenberg, A., 2017. Technosystem. Harvard University Press.

Felt, U. 2015. Keeping Technologies Out: Sociotechnical Imaginaries and the Formation of Austria's Technopolitical Identity, In. (ed) Sheila Jasanoff and Sang-Hyun Kim Dreamscape of Modernity. Sociotechnical Imaginaries and the Fabrication of Power. Chicago and London: The University of Chicago Press.

Fink, A. 2020. Walking on Broken Glass: The Challenges of 2020's Arms Control. Retrieved 23 March 2020, from https://www.europeanleadershipnetwork.org/commentary/walking-on-broken-glass-the-challenges-of-2020s-arms-control/, accessed 21.03.2020.

Frenkel, S. 2018. Microsoft Employees Protest Work With ICE as Tech Industry Mobilizes Over Immigration. The New York Times. June 19, 2018, from https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html, accessed 21.03.2020.

Fukayama, F. 2009. Transhumanism. Foreign Policy. Sourced at: foreignpolicy.com/2009/10/23/transhumanism

Geissler, E. and van Courtland Moon, J.E. eds., 1999. Biological and toxin weapons: research, development, and use from the Middle Ages to 1945 (Vol. 18). Oxford:: Oxford University Press.

Gantz, V. M., Jasinskiene, N., Tatarenkova, O., Fazekas, A., Macias, V. M., Bier, E., & James, A. A. (2015). Highly efficient Cas9-mediated gene drive for population modification of the malaria vector mosquito Anopheles stephensi. Proceedings of the National Academy of Sciences, 112(49), E6736-E6743.

Gardner, D. 2020. Defense Research Contributes to Ebola Vaccine Effort. U.S. Department of Defense. https://www.defense.gov/Explore/Inside-DOD/Blog/Article/2064716/defense-research-contributes-to-ebola-vaccine-effort/

Godet, M. 1994. From Anticipation to Action - A Handbook of Strategic Prospective

Hoffman, D. E. 2012. Genetic weapons, you say? Foreign Policy. March 27, 2012, https://foreignpolicy.com/2012/03/27/genetic-weapons-you-say/

International Committee for Robot Arms Control (ICRC). 2018. Open Letter in Support of Google Employees and Tech Workers. Available at https://www.icrac.net/open-letter-in-support-of-google-employees-and-tech-workers/ accessed 28.03.2020.

Kamradt-Scott, A., Harman, S., Wenham, C. and Smith III, F., 2015. Saving lives: the civil-military response to the 2014 Ebola outbreak in West Africa. The University of Sydney.

Jasanoff, S. ed., 2004. States of knowledge: the co-production of science and the social order. Routledge.

Jasanoff, S. and Kim, S.H. eds., 2015. Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power. University of Chicago Press.

Kloppenburg, S., & Van der Ploeg, I. (2020). Securing identities: biometric technologies and the enactment of human bodily differences. Science as Culture, 29(1), 57-76.

Kania, E. 2017. Battlefield Singularity. Artificial Intelligence, Military Revolution, and China's Future Military Power. Report CNAS. https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power

Leander, A & Wæver, O (eds). 2019. Assembling Exclusive Expertise: Knowledge, Ignorance and Conflict Resolution in the Global South. Worlding Beyond the West, Routledge, Abingdon.

Lentzos, F. 2018. How do we control dangerous biological research? April 12, 2018. Bulletin of the Atomic Scientists. https://thebulletin.org/2018/04/how-do-we-control-dangerous-biological-research/

Lentzos, F., Littlewood, J. 2018. DARPA's Prepare program: Preparing for what? July 26, 2018. Bulletin of the Atomic Scientists. https://thebulletin.org/2018/07/darpas-prepare-program-preparing-for-what/?utm_source=Twitter&utm_medium=Twitter%20Post&utm_campaign=DARPA_July26

Lindblom, C. E. 1959. The science of muddling through. Public Administration Review, 19, 79–88.

Lodgaard, S., 2019. Arms Control and World Order. Journal for Peace and Nuclear Disarmament, 2(1), pp.1-18.

Magnani, L. 2004. "Model-Based and Manipulative Abduction in Science", in Foundation of Science 9.
Magnani, L. 2009. Abductive Cognition - The Epistemological and Eco-Cognitive Dimensions of Hypothetical Reasoning.

Mankoo, Alex and Rappert, Brian, eds. 2018. Chemical Bodies: the techno-politics of control. Geopolitical Bodies, Material Worlds. Rowman & Littlefield, London; New York.

Masco, J., 2006. The nuclear borderlands: The Manhattan Project in post-cold war New Mexico. Princeton University Press.

Masco, J. 2017, Nuclear Technoaesthetics: Sensory Politics from Trinity to the Virtual Bomb in Los Alamos In McCarthy, D.R. ed., Technology and world politics: An introduction (pp.103-124). Routledge.

McCarthy, D.R., 2013. Technology and 'the international' or: How I learned to stop worrying and love determinism. Millennium, 41(3), pp.470-490.

Merom, G., 2001, "Forecasting the Future of War: Foundations for an Algorithm", in Maoz, Z. and Gat, A., eds, War in a Changing World.

Mehta, P. K., Bess, C., Elias-Smale, S., Vaccarino, V., Quyyumi, A., Pepine, C. J., & Bairey Merz, C. N. (2019). Gender in cardiovascular medicine: chest pain and coronary artery disease. European Heart Journal, 40(47), 3819-3826.

Millett, P., Binz, T., Evans, S.W., Kuiken, T., Oye, K., Palmer, M.J., der Vlugt, C.V., Yambao, K. and Yu, S., 2019. Developing a comprehensive, adaptive, and international biosafety and biosecurity program for advanced biotechnology: The IGEM experience. Applied Biosafety, 24(2), pp.64-71.

Munich Security Conference. 2020. https://securityconference.org/en/medialibrary/asset/conversation-corporate-responsibility-to-protect-the-politics-of-big-data-20200215-1730/

The National Academies of Sciences, Engineering and Medicine. 2017. A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology. Interim Report. Available at https://www.nap.edu/catalog/24832/a-proposed-framework-for-identifying-potential-biodefense-vulnerabilities-posed-by-synthetic-biology

O'Brien, C., 2020. EU Introduces AI Strategy To Build 'Ecosystem Of Trust'. VentureBeat. https://venturebeat.com/2020/02/19/eu-introduces-ai-strategy-to-build-ecosystem-of-trust/amp/?__twitter_impression=true [Accessed 20 March 2020].

Paavola, S. 2006. On the Origin of Ideas: An Abductivist Approach to Discovery

Parliament. House of Commons. 2018. Disinformation and 'fake news'. (HC 1719 (111)). London: House of Commons.

Pasgaard, M., Van Hecken, G., Ehammer, A., Strange, N., 2017 Unfolding scientific expertise and security in the changing governance of Ecosystem Services, Geoforum (84) 354-367.

Project Alpha. 2020. Catalogue of case studies on intangible technology transfers in academia and research institutes https://t.co/4l32YDXSdN?amp=1

Reeves, R.G., Voeneky, S., Caetano-Anollés, D., Beck, F. and Boëte, C., 2018. Agricultural research, or a new bioweapon system? Science, 362(6410), pp.35-37.

Roberts, S., L., and Elbe, S. 2016 Catching the flu: Syndromic surveillance, algorithmic governmentality and global health security. Security Dialogue, 48 (1). pp. 46-62.

Rothe, D. 2016. Securitizing global warming. A climate of complexity.Routledge studies in resilience. London: Routledge.

Robinson, J. P. 1998. Contribution of the Pugwash Movement to the International Regime Against Chemical and Biological Weapons, available at http://www.sussex.ac.uk/Units/spru/hsp/documents/pugwash-hist.pdf.

Sackman, H. 1975. Delphi Critique: Expert Opinion, Forecasting and Group Process. Lexington Books.

Sutherland, W. J. and Woodroof, H. J. 2009. The Need for Environmental Horizon Scanning', Trends in Ecology and Evolution, 24(10), pp. 523–527.

Stirling, A., O'Donovan, C. and Ayre, B. 2018. Which Way? Who says? Why? Questions on the multiple directions of social progress. Technology's Stories. pp. 1-20.

Virilio, P., 1989. War and cinema: The logistics of perception. Verso.

Weisgerber, M., 2020. General: Project Maven Is Just the Beginning of the Military's Use of AI. Defense One. https://www.defenseone.com/technology/2018/06/general-project-maven-just-beginning-militarys-use-ai/149363/ [Accessed 28 March 2020].