CTRL + power: the (geo)politics of digital authoritarianism

2024 Report

A symposium organised by LSE IDEAS and T.wai - Torino World Affairs Institute, in cooperation with Department of Cultures, Politics and Society of the University of Turin

In memory of Professor Cristopher Coker

As is often the case, the symposium started with organizers expressing their gratitude to the institutions and individuals that made the event possible. In 2024, however, the symposium was dedicated to the late co-director of LSE IDEAS, Professor Christopher Coker, who passed away in September 2023. The first few words of co-organizers Stefano Ruzza and Chris Alden honour his memory:

Professor Coker was instrumental in making today's event possible. He spent much of his life exploring the intersection of technology, humanity, and society. We owe much to his intellectual legacy and to the insightful conversations we had with him on the very same topics we are discussing in this symposium.

This event represents only the latest expression of a deeper cooperation between Turin-based research institutions and LSE IDEAS, a partnership Professor Coker forged and had actively promoted since 2013. This symposium embodies his remarkable institutional legacy.

Last, but by no means least, Professor Coker's personal legacy endures in the relationships he fostered through his very personal style of engaging with arguments and people. Though Professor Coker is not with us in person, his influence permeates all our discussions.

In many ways, today's event is dedicated to our colleague and old friend Christopher.

On 6–7 May 2024 the London School of Economics' think tank LSE IDEAS; the Turin-based think tank T.wai – Torino World Affairs Institute; and the Department of Cultures, Politics and Society of the University of Turin held their fourth joint international symposium.

Titled 'CTRL + Power: The (Geo)Politics of Digital Authoritarianism' and organized over two days, the symposium featured thematic panels and conversations between renowned scholars, early-career researchers, and practitioners.

Day 1

Day 2

Opening remarks

The 2024 edition of the joint symposium builds on the premise that governments are increasingly aware of how the digital domain can be leveraged to both support and undermine the stability of their regimes, whether these are considered democratic or authoritarian. Yet, as **Stefano Ruzza** highlights, the latter:

> have shown a strong capacity to adapt and use digital and emerging technologies to preserve and expand their authoritarian traits in various ways, from silencing domestic opposition and curtailing protests through blunt internet shutdowns, to manipulating international public opinion and interfering in foreign elections through troll farms.

These are just a few of the digitally enabled tools and tactics at the disposal of the authoritarian and hybrid (i.e. partly authoritarian) regimes that this symposium seeks to interrogate.

Relatedly, the symposium also focuses on what **Chris Alden** refers to as 'the "currency of information" in our digital world – a currency increasingly questioned in what some call a "post-truth" era, where empirical facts, once clear, are now blurred and contested'. As Alden goes on to explain:

> this shift challenges our ability to make sense of the world, much as disinformation did during the Cold War. Looking back to the 1960s, the Soviet strategy of identifying the vulnerabilities of liberal states and exploiting them to bend the truth offers a historical parallel to today's digital environment whereby open societies are turned into fertile ground for disinformation and manipulation.

Applying our historical memory to the contemporary digital environment, Alden argues, prompts us to 'ask big questions, not just about politics but about the ethical challenges of our time: what does a "post-post-truth" world look like, and how do we navigate this complex landscape?'.

Thus, Ruzza summarizes, 'the symposium aims at exploring the darker side of the digital world, focusing on the political dynamics of digital authoritarianism that emerge from the interplay of national and international influences'.

Against this backdrop, participants in this symposium are invited to reflect on the options available to policymakers and practitioners to mitigate and counter the impact of digital forms of authoritarian influence and resilience. Indeed, as **Nicolò Russo Perez** also points out:

> many local challenges to democracies and democratic processes – such as the erosion of social cohesion and increased perceptions of insecurities – are rooted in global issues. Our solutions thus need to start from a broader understanding of the origins of phenomena such as those addressed by this symposium: the digital realm, inherently global, has local impacts. It is a 'glocal' issue.

And as such, Russo Perez concludes, it requires innovative public policies informed by rigorous research and by the kind of discussions and exchanges that spaces like this symposium allow, thanks to the support of private institutions such as the Fondazione Compagnia di San Paolo.

Keynote speech

by Anja Kaspersen

The following text is based on a speech given by Anja Kaspersen at the start of the symposium.
The speech was subsequently shaped into this publication by T.wai – Torino World Affairs Institute.

The late Professor Christopher Coker's impact on the fields of international relations and military studies is profound. Beyond his being my mentor, his influence profoundly shaped my thinking and professional trajectory. Coker was a visionary thinker and an astute observer of history and the people striving to coexist within it. While he is frequently associated with his work on warfare, his understanding of technology, computational research, and digital anthropology is equally deep and significant. His ability to delve into the subtle, often unspoken forces that shape society – captured by concepts such as *doxa*, as articulated by sociologist Pierre Bourdieu, and 'social silences', as discussed by anthropologist Gillian Tett – was central to his intellectual approach. He understood that these powerful, unspoken forces often convey more than the noisy social babble. Coker's mastery of listening is a human quality that has become increasingly vital in today's noisy digital age. His ability to demonstrate not just insights but actual foresight across the natural and social sciences and the humanities, with such ease that it left the rest of us in awe, made him a unique polymath and thinker. He knew all too well that what happens in society, in politics, and on the battlefield is inextricably linked with our humanity.

Coker's views on technology, particularly in the context of warfare, align closely with the insights of Ursula M. Franklin, a scientist and renowned thinker on the social impacts of technology. Franklin observes that 'Technology is a *system*. It entails far more than its individual material components. It involves organisation, procedures, symbols, new words, equations, and, most of all, a mindset'. Both Coker and Franklin understood that technology is not merely a collection of tools and devices but a complex, deeply embedded system that shapes how we live, think, interact, and perceive the world – a precursor to what we now recognize as socio-technical systems. However, especially in the context of artificial intelligence (AI) systems, one could argue whether these are truly techno-social systems, as the term implies an equilibrium between technological influence and social structures, whereas reality often shows a dominance of technological imperatives over social ones.

Coker believed that humanity's relationship with war, and by extension the technologies we develop and use to fight war, offers profound insights into what it means to be human. In his book *Humane Warfare* (2001), he argues against the illusion that technology can make war more humane. Despite technological advancements, Coker cautioned, the brutality of war persists and may even be exacerbated by these so-called 'humane' technologies: 'The idea that technology can remove the horror of war is as dangerous as it is naïve. War, at its core, is about human conflict, and no amount of technological sophistication can sanitise that reality.' These insights resonate deeply in today's discussions about AI in warfare, where certain applications of AI threaten to either depersonalize or hyper-personalize, thereby obscuring the true costs of war. Coker noted that the wars of the future, often envisaged by the promise of digital technologies and AI, involve 'the abstraction of war's ugliness by making it a digitalised phenomenon'. However, he never shied away from emphasizing that war is anything but a computer game, and life, above all, is a complex endeavour, not one that lends itself easily to computation in any way or form – nor should it. His writings reveal a significant and expanding mind, and demonstrate how farsighted he was in his scholarship, perhaps developing as a result an intense distaste for hubris and false pretences.

In *Future War* (2015), Coker provocatively asks whether machines will gradually 'come to be seen not as replacements for human beings but as extensions of our own humanity'. Coker often discussed the importance of the 'warrior ethos' – a set of principles and values that have historically defined the conduct of soldiers. He was concerned that AI and other advanced technologies might fundamentally change this warrior ethos. Traditionally, warriors have been guided by principles of honour, bravery, and ethical conduct, all of which are deeply intertwined with the human experience of combat. However, as warfare becomes increasingly automated and remote, there is a risk that these values could be eroded. The distance provided by, for example, drones and AI systems not only allows decisions to be made far from the battlefield but also enables the formation of new battlefields altogether, potentially disconnecting and alienating the human element from the violence and consequences of those decisions.

In his essay 'Artificial Intelligence and the Future of War', Coker asks:

> If war becomes increasingly dependent on technology, what of individual agency? Is war slipping out of our hands? How long will we continue to 'own' it? Agency is a tricky business – it is framed by the stories we tell ourselves, as well as others.

He acknowledges that:

> AI is not going to change war for some time yet. What it will do is further amplify the way war will be driven by technological drivers (i.e., our own relationship with machines as we become increasingly absorbed into them, and they into us – the man/machine symbiosis, or what is often called the 'post-human condition').

This point is also emphasized by the international law scholar Kobi Leins, who writes that 'science initially developed to benefit mankind is often co-opted in war. Many scientific developments undertaken for unrelated purposes have been reappropriated for use in warfare'. This 'reappropriation' is particularly evident in the field of AI. Leins also stresses the urgent need to 'collaborate, clarify parameters of use, prevent dual use, and identify the appropriate timing for legal review' before these technologies are embedded into core functions of public governance. This observation aligns with the broader context of military systems evolution, where new technologies, such as AI, are incorporated into military capabilities. The challenge lies in the fact that the impact of any particular scientific technique or technological system on military affairs is not a given. AI applications have advanced in areas such as autonomy, robotics, and decision support, yet their progress is generally broader than it is deep, and their integration into transformative military capabilities remains nascent. This lack of depth highlights the complexities and uncertainties involved in adopting AI within military systems, echoing the cautionary views of Coker and others.

One could also surmise that the 'warrior ethos' has a technological counterpart; the 'systems developer ethos' might be one way of looking at it. Some of the same trains of thought, reflected not least in the work of Yoshua Bengio and Stuart Russell, two senior figures in the field of machine and deep learning, echo the questions asked by Coker. Just how long will we be able to continue to own AI systems and models? Is AI slipping out of our hands? And where are the decision-makers, leaders, and others in this? What is their ethos – the 'leadership ethos'? For leaders and decision-makers, there is a cost to being concerned. Sarah Hooker, a machine-learning researcher, wrote with great clarity that 'Machine-learning researchers do not spend much time talking about how hardware chooses which [and, I would add, whose] ideas succeed and which fail. This is primarily because it is hard to quantify the cost of being concerned'. Exactly what is the cost of being concerned? Perhaps we need to measure the costs of being concerned and balance them against the current mantra of return on investment at any cost. Otherwise, we end up with a return on indifference.

My point being: every culture, every tribe, every group has an ethos. What stories are we telling ourselves, exactly, and who gets to tell them? The vernacular and words that get shaped in the process matter. They matter for how we govern and for how we perceive what is at stake. Otherwise, we too often end up in binary propositions of the world that serve little to no purpose if the focus is to ensure that powers are kept in check and negative impacts are held at bay through regulations and standards. There is no evil or good AI; these are just framings.

This new state of accounting with the technological genie raises critical questions about whether AI is changing the warrior ethos in ways that Coker would have found deeply troubling. If the warrior's role becomes more about managing machines and less about direct engagement, does this diminish the sense of responsibility and ethical reflection that has traditionally been central to the concept of the 'warrior'? Coker feared that the increasing reliance on technology might lead to a form of moral distancing, where the horrors of war are obscured by the very technologies designed to make warfare more efficient. In the words of Coker: 'In making war more humane for ourselves, do we make it less human for everyone else? In the end, the question is an ethical one.' Ethics, Coker opines, is 'carefully crafted, in other words, not by abstract philosophy alone, but by practical action'. Unfortunately, as war becomes more technological, it is 'distancing public opinion and the warrior from its consequences' and raising this question: 'Will it make us more prone or less prone to wage it?' This moral distancing – creating separation from the victim but increasing rapprochement with the machine – suggests that a new form of ethics may emerge from human–machine interaction. Coupled with political cowardice in addressing the ethical implications of such technologies, this threatens to erode the foundational values that have historically guided human conduct in conflict.

This also raises fundamental ethical questions about whether new technologies in warfare are making war more humane or, paradoxically, more brutal. As we integrate AI into the battlefield, are we reinforcing ethical constraints, or are we enabling a kind of violence that is further removed from human empathy and moral reflection? Historically, technologies have often intensified the inhumanity of war by stripping away the very ethical frameworks that guide human conduct in conflict. Today, the relentless pursuit of technological advantage and prowess has surpassed the traditional frames and paradigms of governance and oversight, leaving much to the technological forces at play.

Coker's insights into the silent forces at play in society become especially pertinent when we consider the rise of AI and digital technologies in society. Just as Coker listened for what was left unsaid in human interactions, we must carefully examine the intentions of those who invest in, develop, deploy, and oversee these technologies – focusing not only on what they choose to amplify but also on what they might suppress or overlook.

In our digital age, what is left unspoken often carries the most powerful storylines. While AI and digital technologies promise to transform our lives, we must critically ask: at what cost, who decides, and through what approach?

Concerns about the erosion of ethical frameworks are not limited to warfare. They extend to the broader societal implications of AI and other emerging technologies. As AI systems become more integrated into our daily lives, they raise fundamental ethical questions about whether these technologies are making our society more humane or, paradoxically, more brutal. Are we reinforcing ethical constraints, or are we enabling a kind of behaviour that is further removed from human empathy and deep reflection?

This question of AI's impact on society is further complicated by the reductionist approach often taken in the development and deployment of these technologies. By reducing complex human behaviours, thoughts, and social dynamics to mere data points and computational problems, we risk oversimplifying the essence of what it means to be human. This reductionist view fails to account for the rich, nuanced, sometimes painful, and often unpredictable nature of human life, which cannot easily be captured by algorithms or data models. It tends to favour and promote a narrative of technology as a panacea for all societal issues.

AI employs mathematical and probabilistic machine-learning models, such as deep learning, to generate outputs that *mimic* human engagement. However, these systems lack the contextual sensibilities and symbolic logic inherent in human thought. At the core of many AI systems, especially those relying on deep learning, are complex networks designed to process vast amounts of data, often referred to as neural networks. These networks can generate new data instances, such as images, text, or audio, that bear an uncanny resemblance to the data on which they were trained. Generative AI models, while impressive in producing content that mirrors their training inputs, remain confined to these pre-defined parameters. They produce outputs based on patterns found in the training data but lack the capacity for understanding. This limitation is particularly evident in their tendency to produce what are known as fabrications (hallucinations) – outputs that, while plausible on the surface, are incorrect or nonsensical on closer inspection.

Gary Marcus, a cognitive scientist and AI researcher, observes that 'We've been seduced by the success of deep learning into thinking it's the whole story, but it's just one piece of the puzzle'. Moreover, treating AI as a monolithic entity that can be uniformly regulated and governed overlooks the diverse and nuanced challenges posed by different AI systems. Furthermore, these challenges profoundly impact how we engage with and address potential and inherent harms. Will Douglas Heaven, a tech journalist, recently highlighted that 'AI has come to mean all things to all people, splitting the field into fandoms. It can feel as if different camps are talking past one another, not always in good faith'.

I welcome the diversity of views and believe that the best collective intelligence comes from being able to navigate differences and fiercely questioning the notion that nothing is inevitable. As with most things in life, in politics, in the exercise of democracy, in war and in peace, it comes down to a very human endeavour: seeking definitions and decisions, and grappling of necessity with their outcomes, impacts, and trade-offs. In life, the only certainty is that things will evolve and paradigms will change. But without awareness, without consent, without a public conversation, this is simply not tenable. And as regards AI – however one defines it or wherever one finds oneself on the belief cycle of what it is and what we want it to be – one thing is sure: there are and will be trade-offs, by design and by default.

Actual definitions of and perspectives on what AI is – what it represents and constitutes – are as varied and complex as the number of researchers in the field. And that is okay. It is the ethics part I worry about, as varied and complex interpretation of ethics risk becoming a tool of evasion rather than a tool of non-harmful engagements with our lived environment becoming a tool of evasion rather than a tool of non-harmful engagements with our lived environment. For AI, it is important to have definitions for the purposes of regulation, validation, verification – but for the purpose of scientific curiosity, it is healthy to allow many viewpoints to arise and cross-fertilize.

The endeavour of replicating human-like intelligence through computational methods focuses on the capacity of AI systems to process data, recognize patterns, and perform tasks that traditionally require human intelligence. This view sees AI as a sophisticated tool for enhancing and automating tasks across various domains. Others, however, take a broader view, defining AI as a technique and approach for organizing the vast quantities of data generated every millisecond. This perspective emphasizes AI as a tool of power, used not only to automate processes but also to influence, control, and shape societies. This understanding of AI as a mechanism for power aligns with the notion that AI could be seen as 'power through other means', and 'humans as cogs in the machine', echoing the ideas of strategic thinkers such as Wiener and Clausewitz, which Coker often humorously paraphrased. Andrew Bard Schmookler aptly captures this sentiment: 'In the hands of the powerful, AI has become a new means to manipulate, surveil, and control societies, shaping not just our actions but our very perceptions of reality.' Still, others critically evaluate AI's current limitations in understanding, questioning whether it can ever truly replicate the deeper, more nuanced aspects of human cognition, such as moral judgement, contextual awareness, and symbolic reasoning.

These differing perspectives reflect the significant challenge in providing a clear and universally accepted definition of AI. For some, AI is a powerful tool capable of advancing technology and solving complex problems, while others see it as fundamentally limited and potentially dangerous in its current form.

What is undeniable is that AI's effectiveness and impact are highly context-dependent – shaped by the data it is trained on, the people who build and train these models, the level of computational resources available, and the scientific and ethical approaches chosen. As Francesca Rossi, an AI researcher, points out, 'AI is not just about algorithms and data; it's about understanding how these systems will interact with the world and with society'. This nuanced understanding is crucial, as it also helps in recognizing that the approach or method of verification you choose to procure or acquire and embed in your country, organization, or company is important – and often overlooked or not properly understood.

The challenge of our time is to recognize AI's limitations, despite the sloganeering; understand its diverse applications and implications; and avoid the temptation to treat it as a catch-all solution. In the words of Coker, 'algorithmic thinking is not necessarily the best way to deal with reality, and not all problems are computational, even those to which we think we know the answer'. Like Coker, Gary Marcus argues that 'True intelligence is not just pattern recognition; it involves reasoning, understanding of cause and effect, and the ability to adapt to new and unforeseen situations'.

My goal here is not to provide ultimate answers but to leave you with meaningful questions and material for further contemplation.

One important dimension to consider is the notion of errors when engaging with systems that far surpass our ability to process information. Some argue that by embedding more AI and continuously deploying it, we may reduce errors and increase accuracy. However, it is more accurate to say that AI produces different kinds of errors – errors that our societies are not yet equipped to respond to, as they are simply beyond human comprehension and planning capabilities. This is particularly important in a military setting. This challenge is amplified with the advent of generative AI systems and large language models, where the complexity of these systems further complicates our ability to foresee and mitigate potential issues. As Paul Scharre notes, 'AI can be remarkably precise, but precision without context is dangerous. Fewer errors in one domain may lead to catastrophic failures in another'.

These errors, along with the methodologies behind them, shape not only how we view the world but also the world we ultimately create, influencing who and what we prioritize. Missy Cummings, a roboticist and a leading expert on autonomous systems, warns of the dangers of over-reliance on AI, stating that 'The biggest risk of AI is that it encourages overconfidence in its capabilities. We have to remember that these systems are far from infallible and require human oversight to ensure they don't lead us into unforeseen problems'. Sarah Hooker elaborates on this by discussing the 'hardware lottery', where many algorithms succeed not because they constitute the right approach but because they are the right fit for the available hardware. This phenomenon highlights a crucial issue: the interaction between AI systems and the physical and computational environments in which they operate can lead to unintended consequences, particularly when those systems are deployed without a full understanding of their limitations. Furthermore, AI systems' troubling tendency to 'fabricate' underscores the risks of relying too heavily on such models. Without a new architectural approach adopting a safety-first principle that moves beyond current paradigms, the risks associated with AI far outweigh its promises.

Both Cummings and Pascale Fung, although from different scientific backgrounds

– Cummings in robotics and autonomous systems, and Fung in computational linguistics and AI – have expressed significant concerns about the ethical implications and risks associated with AI technologies. Pascale Fung has highlighted the dangers of deploying AI without sufficient oversight, particularly the potential for AI systems to amplify misinformation and other societal harms. Missy Cummings, meanwhile, has specifically addressed the brittleness of AI systems, noting that these systems can perform well under specific conditions but are prone to catastrophic failures when those conditions change unexpectedly. This brittleness makes AI systems particularly vulnerable in dynamic environments, underscoring the necessity of human oversight, which must be supported by strong verification processes and investment in human skills to effectively manage and mitigate these risks.

Joanna Bryson, like Franklin before her, has said that 'AI is not an artefact; it is a tool that reflects the values and decisions of those who create and deploy it'. This idea aligns closely with Coker's scholarship on technology's impact on war and humanity. He frequently opined that technology, including AI, is an extension of our expressed and overt ambitions. Technology does not simply change the world around us; it changes us by extending our capacities, altering our perceptions, and reshaping our social interactions. The development and deployment of AI are not neutral acts but are deeply intertwined with our political, ethical, moral, and (increasingly) economic frameworks. Moreover, these systems are not without significant environmental costs, given their reliance on vast volumes of data and energy-intensive processes.

One valuable book Coker shared with me is Barbara Ehrenreich's *Blood Rites* (1997), which explores the militarization of society and the human condition, offering profound insights that resonate with Coker's scholarship. Ehrenreich examines the primal and ritualistic aspects of war, providing insights into how these deep-seated behaviours and beliefs continue to shape modern conflicts and the direction of military innovation. These cultural beliefs and rituals help determine not only the conduct of war but also what societies deem worth investing in, from advanced weaponry to emerging technologies. Coker admired Ehrenreich's ability to blend history, anthropology, and social critique to reveal the underlying forces driving human behaviour, particularly in the context of war. He would often reflect on her observation that 'men will kill for an idea, provided they don't have to pay the price', linking it to the growing detachment facilitated by technological advances in warfare.

This concern is further amplified by the insights of Josef Weizenbaum, a computer scientist and the creator of the first language-processing computer program, ELIZA, who cautioned against the 'god-like' reliance on computational systems. Weizenbaum warned of the risks of disconnecting from human-centric values, stating that 'There are certain tasks which computers ought not to be made to do, independent of whether computers can be made to do them'. His perspective underscores the danger of assuming that technology can replace human judgement and ethical reasoning in areas where these qualities are essential.

Wendell Wallach, a leading thinker on technology and ethics and co-author of *Moral Machines* (2009) and author of A Dangerous Master (2015), also underscores the need for a new ethical framework and even a new paradigm suited to the challenges posed by AI and other advanced technologies. He argues that ethical concerns should not be an afterthought but rather a guiding principle in the development and deployment of technology. This approach is crucial for ensuring that technology serves humanity rather than undermining it. He posited that we must acknowledge any and all trade-offs and manage them carefully to navigate the complexities of technological advancements effectively. This perspective on 'trade-off ethics' aligns with Coker's idea that ethics is crafted by 'practical action'. Trade-off ethics, according to Wallach, 'entails looking at each possible course of action and weighing [its] benefits and risks before deciding what action to take'.

The implications of AI's influence on society extend far beyond technical concerns. Langdon Winner, a political theorist and philosopher, famously argues that 'artefacts have politics', meaning that technologies are not neutral tools but carry within them the power structures and intentions of those who create and deploy them. This insight aligns closely with Coker's observations on the ethical and societal implications of technological advancements, particularly in warfare. The assumption that technology can remain neutral in its development and application ignores the broader social and political contexts in which these technologies are deployed.

Hannah Arendt's exploration of the dangers of lying in politics is particularly relevant in this context. I am deeply grateful to Coker for introducing me to Arendt's works, which have significantly shaped my intellectual orientation – almost as much as Coker's own insights. In her exceptional essay *On Lying and Politics* (2022), Arendt argues that when lies consistently replace factual truth, it leads not only to deception but also to the erosion of a society's ability to distinguish between truth and falsehood – an ability that is foundational for any functioning society. In today's digital age, AI could exacerbate this issue by enabling the creation of tools that not only disseminate misinformation but also manipulate reality itself, leaving societies increasingly vulnerable to manipulation by authoritarian mindsets. The indifference towards the distinction between truth and falsehood in this landscape is especially troubling, contributing to a culture where truth becomes increasingly malleable. She argues:

> The result is not that lies will now be accepted as truth, and the truth defamed as lies, but that the sense by which we take our bearings in the real world – and the category of truth versus falsehood is among the means to this end – is being destroyed.

Arendt's concept of the 'banality of evil' is also highly relevant in the context of AI. She argues that some of the greatest evils in history were perpetrated by ordinary individuals who simply followed orders and conformed to societal norms without questioning the profound impact of their actions. As Arendt has famously observed, evil can be committed by those who neither deeply reflect on their actions nor intend harm, but who simply carry out their duties within a system. In the digital age, AI systems could mask harmful actions on a massive scale while distancing those responsible from the ethical consequences of their decisions through layers of technological abstraction. These are concerns central to Coker's apprehensions about how technologies and techniques are embedded within societal structures lacking any clear 'leadership ethos'. This raises urgent concerns about how these systems are made capable of automating not only the banality of evil but also radicalization (of any views), making it crucial to engage in rigorous ethical and public scrutiny.

Responsibility becomes paramount. Politicians, too, are increasingly asked to make critical decisions about what and how much to invest in AI technologies that are being built and embedded across society. In the future, they might claim that they did not fully understand the techniques and technological methods in question and thus were not equipped to foresee the broader consequences. The abdication of responsibility, whether intentional or due to a lack of understanding, echoes the danger Arendt warned of – the risk of enabling harmful actions through uncritical acceptance and a failure to scrutinize the deeper ethical implications of those decisions.

Coker's concern about the erosion of truth is further amplified in the context of AI, where the automation of decision-making risks normalizing behaviours and choices that might otherwise be challenged, leading to a quiet erosion of societal integrity, human dignity, equality, and – ultimately – to silence. Yet, Coker also firmly believed in the role of our contemporary academic institutions in opening up a space for 'post-truth' through an embracing of relativism. He saw value in being able to sit with multiple truths at the same time, not viewing them as conflicting but rather as an opportunity to understand something deeper. This reflected his interest in Nietzsche, who also grappled with the complexities of truth, perspective, and the multiplicity of meanings in life.

A keen observer of Nietzsche's scholarship, Coker often reflected on the philosopher's insights into how our tools shape our thoughts and, by extension, our society. Anyone who spent time with Coker would have encountered a few Nietzsche quotes. One that he shared with me was '*Sie haben Recht: Unser Schreibzeug arbeitet mit an unseren Gedanken*', which translates to 'You are right: our writing tools work to shape our thoughts'. This idea captures the essence of the profound impact that the tools and technologies we create have on our cognition, decisions, and, ultimately, our societies. Nietzsche's perception links strongly to Langdon Winner's insights that 'artefacts have politics' and Coker's scholarship examining the technologies we develop, not only for their immediate utility but also for their broader, long-term implications for our collective consciousness and social fabric.

As I reflect on these issues, given the focus of this conference, it becomes clear that unchecked technological advancement could lead to significant societal harm and authoritarian misuse, both intentional and accidental. For example, the development and deployment of AI-driven surveillance systems in public spaces, justified under the guise of public safety, can easily shift from protecting citizens to controlling and monitoring them in ways that stifle freedom and autonomy, and ultimately cause harm. This is particularly concerning given that many large AI systems and models are being developed by private actors without adequate scrutiny and are embedded without sufficient safeguards or verification of their integrity.

As Coker might have asked, does it matter whether the harm is intentional or accidental? In either case, the way is paved for these technologies to be used in ways that do not serve basic principles of human rights, non-oppression, public space ethics, and public transparency, even in the democratic states where such technology is increasingly being adopted. Adding to this concern, I would like to repeat a critical question: who decides, and to what end? In an AI-driven world, the distinction between intentional and accidental outcomes becomes even more pressing as the decision-making process grows increasingly opaque. The risk is that decisions made by equally opaque AI systems, guided by unseen algorithms and vast data sets, could lead to outcomes that are neither transparent nor accountable, eroding the moral and ethical frameworks that should guide our societies. This is why Arendt's argument remains so relevant today – it challenges us to remain vigilant, questioning not just the technology itself but also the intentions, processes, and impacts it creates in the hands of powerful entities, or 'juggernauts', as Wendell Wallach calls them.

To illustrate and demonstrate the need to hold technology companies accountable, consider the global tech sector's mixed progress on delivering 'voluntary commitments' to AI safety, which reveals significant caveats. This is particularly disturbing given what we have learned about the vast implications of faulty procedures for testing software safety. The limitations of self-regulation as a governance tool should concern decision-makers everywhere. Some good practices have emerged in recent years, but they are nowhere near where they need to be in terms of comprehensive governance or the protection of rights at large. Complicating matters further, in my experience, is the large elephant in the room regarding whether platforms and technology companies, and the services they provide, function as public utilities, despite not being public utilities. Often, we hear that they are 'global, private enterprises' and therefore not subject to such requirements. But just because something is repeated often does not mean it is true. We have already regulated other critical infrastructure essential to public safety, human dignity, and international security, so why not these companies?

There are many valid opinions, and just as AI is not a singular entity and is different things to different people, there is significant uncertainty about whether this is a right and feasible course of action. This is compounded by a perception that if we do not do it, someone else will, and no one wants to 'miss out' or 'fall behind'. The question then becomes whether decisions made today will hinder or promote innovation, rather than asking whether thoughtless decisions today will create new threats and less security. The greatest challenge, as I see it, is that the major players in the technology field are not just one thing, and with significant AI investments the complexity increases. Historically, attempts at regulation have often failed when there is uncertainty about the roles of these companies – an uncertainty that is often intentionally created or maintained to avoid regulation. Meredith Whittaker has repeatedly highlighted the danger of 'regulatory capture' amid all the hype, absent governance and lack of a 'leadership ethos'.

We must, therefore, ask the right and sometimes uncomfortable questions and draw historical parallels with the current situation. While comparisons are often made with industries like tobacco or oil, these analogies fall short due to the multifaceted nature of tech companies. A more relevant historical example is the United Fruit Company – a corporation that once wielded significant influence over political and economic systems in Latin America. This case illustrates how corporate power can have wide-reaching impacts on public welfare. Similarly, modern tech companies possess the capability to shape global information flows and public opinion, which highlights the importance of developing international ethical frameworks and fostering transnational cooperation to address these challenges in the digital age.

Moreover, given what we now know about these systems' brittleness, relentless energy-intensive computing requirements, lack of meaningful transparency, and unclear lines of accountability, the progress made is not as robust as needed. Safety and security operations, including 'red team' efforts, which may have improved in quality in recent years, are still often opaque and managed outside the public realm. A few 'neat technical solutions to the messy socio-technical problem that is AI' will not suffice. Nor will an overt focus on hypothetical risks alone. As the old adage goes, actions speak louder than words. As mentioned earlier, there is nothing inevitable about these technologies if we have the collective courage to engage with the tension points, govern their development and their impact, and steer their beneficial use. To paraphrase Dag Hammarskjöld: the road is paved with (inevitable) trade-offs. The speed and scale at which we embed AI into public governance, critical systems, and our children's imaginary and real lives, blurring the difference between them, are significant. In the process, we may just be forced to come to terms with who we truly are.

I would be remiss if I did not take the opportunity to honour the many people who, over many years, have pooled their collective intelligence to develop better ways to address requirements around safety testing, ethics, security measures, verification, and age-appropriate considerations. There is certainly no shortage of relevant standards as a first step towards greater transparency and confidence-building; what is lacking is the connective tissue. The collective insights, efforts, resources, and talents within and outside the sector are formidable. Indeed, some of the most conscientious individuals working on ethical conundrums are employed by these companies. This observation suggests that many of the issues we see are more a matter of absent leadership and ethical choices than purely technological problems. This underscores the need for more than just voluntary commitments and self-regulation.

Coker often reflected on the paradoxes of modern warfare, observing how technological advancements have fundamentally transformed not only how we engage in conflict but also how we interact with one another as countries, institutions, and individuals. Another scholar whose work influenced his scholarship was Daniel Dennett, a cognitive scientist with deep philosophical insights. Dennett articulated something I heard Coker express concern about many times:

> We really are at risk of a pandemic of fake people that could destroy human trust, could destroy civilization. It's as bad as that. I say to everybody I've talked to about this, 'If you can show that I'm wrong, I will be so grateful to you.' But right now, I don't see any flaws in my argument, and it scares me. The most pressing problem is not that they're going to take our jobs, not that they're going to change warfare, but that they're going to destroy human trust. They're going to move us into a world where you can't tell truth from

> falsehood. You don't know who to trust. Trust turns out to be one of the most important features of civilization, and we are now at great risk of destroying the links of trust that have made civilization possible.

These same ideas permeated Coker's scholarship, where he tirelessly reminded us that no matter how sophisticated our machines become, true peace and human dignity can only be achieved through human effort and understanding.

Coker's work challenges us to continually examine the role of technology in our lives, particularly how it reshapes our understanding of what it means to be human, influences our lived experiences, and alters the way we embody and interpret those experiences. As Emily Bender, a linguist and AI ethicist, suggests, AI is not just a technical challenge but a social one, with deep implications for power and inequality. We must ask ourselves how we can develop and deploy technologies in ways that promote truth, justice, and the common good, rather than furthering division, inequality, and oppression. The ethical challenges posed by AI are not just technical issues but deeply philosophical ones that require us to reconsider the very foundations of our societal structures. It is only through a rigorous, interdisciplinary approach – one that includes the voices of historians, ethicists, anthropologists, mathematicians, and technologists – that we can hope to navigate the complex terrain of AI and other emerging technologies responsibly.

Sherry Turkle adds another important dimension to this discussion by examining how digital technologies can connect us virtually while isolating us emotionally. She warns of a world where we are 'alone together', with technology reducing rich human interactions to mere exchanges. This concern reflects the broader societal challenge of maintaining meaningful human connections in an increasingly digital world, where technology can both bridge and widen social gaps. As loneliness in the digital age grows, it can become a significant problem of national security, particularly as it may be weaponized in clandestine ways. By exploiting social isolation, malicious actors could foster distrust, manipulate public opinion, or even destabilize societies from within, making loneliness not just a personal issue but a potential tool of covert influence.

In conclusion, as we engage with these technologies, it is crucial to remain aware of the ethical trade-offs – or as Wallach describes them, our chosen actions – and strive to ensure that our use of technology enhances, rather than diminishes, our collective human experience. Simply do as Arendt encouraged: stop and think. Coker taught me that the dynamics of AI are not unlike other transformative changes in society; they carry the potential for great benefit but also the risk of unforeseen consequences. These technologies are often developed in anticipation of capabilities rather than in response to clear problems, which can lead to strategic decisions that may create new challenges, exacerbate existing ones, or shift power structures in ways that are difficult to undo.

This situation reminds me of a conversation I had with someone who lived through the 'spiral of losses' at Lloyd's of London in the 1980s. In that case, the repeated reinsurance of the same risks magnified losses across the system, leading to a financial crisis. Similarly, AI technologies, if not carefully managed, could trigger a 'spiral of consequences', where interconnected systems amplify risks and failures, creating a cycle of escalating challenges. This historical example serves as a cautionary tale, reminding us that without careful oversight and ethical consideration, the pursuit of technological advancement can lead to unforeseen and potentially irreversible consequences.

Coker often reflected on the paradoxes of modern warfare, observing how technological advancements blur the lines between war and peace. I often recall a line he shared with me, one I later realized was likely derived from a longer Dickens quote: 'It is in the darkest places that the light must be sought, for it is there that humanity most often reveals itself.' This was Coker's way of guiding me – and perhaps all of us – to find hope and wisdom in the face of complexity, and to remain vigilant, reflective, and humane as we navigate the profound challenges of our time.

PANEL 1

Bad news: assessing and countering disinformation

One of the most disturbing trends accompanying the 'digital revolution' has been the spread of online disinformation and social manipulation through digital means. Yet the roots of these phenomena run deeper and wider than is normally understood, as the symposium's first speaker, **Michelangelo Conoscenti**, underlines.

With the rise of social media, disinformation campaigns are ever easier and cheaper to pull off than in decades past. 'Western societies, especially Europe, are targets of disinformation operations, carried out by well-trained military personnel and', as Conoscenti points out, 'being aware of the fact that key players such as Russia and China are using military techniques is crucial for countering their actions and fostering resilience in our societies'. Indeed, we need a better understanding of how disinformation campaigns rise and spread, of their effects, and of how to stop them from poisoning our information ecosystem and societies. Hence, Conoscenti asks: 'Why is Russian and Chinese dis/misinformation (or, to use a recent European Union (EU) acronym: FIMI, Foreign Information Manipulation and Interference) so successful? Furthermore, how is it that populism, observed as a communicative style, presents, all over the world, strikingly similar communicative strategies as these two authoritarian regimes?'

The World Economic Forum's 2024 *Global Risk Report* (19th edition) names disinformation and misinformation 83 and 74 times respectively, identifying them as the most immediate risks over the next two years. This is a pressing issue: '*Opponents*, who I now acknowledge as such, are actively trying to pollute the public European debate using military information and psychological operations. It must be understood that European public opinion is the target of military operations', says Conoscenti, adding that 'The goal, however, is never, really, to push the election in favour of a preferred candidate. Rather, the real outcome is to slowly chip away at people's belief in political institutions, economic prosperity, social cohesion'. It is, thus, a broader, deep-seated strategy.

While the technology may have changed, disinformation has long been part of the doctrine of Russian and Chinese military information operations. Historically, the Russian Communist Party's newspaper, *Pravda* ('The Truth'), offers a good example of Russia's long-standing disinformation practices. Today, Conoscenti points out, 'Dugin's and Gerasimov's doctrines continue this legacy, with the latter stressing the idea of relative truths and the former aiming to distract' Western societies by exploiting the weaknesses of democratic rule. All of this within a framework on the status of "failed truth and failed democracies" of our institutions'. Importantly, Conoscenti notes, 'whilst NATO considers its information and psychological operations as *wartime* activities, the disinformation efforts of Russia and China are continuous. For them, it is always wartime'.

To support his argument, Conoscenti shares with the audience an audio clip he recorded on Shortwaves in April 2024: two people are conversing in English. They talk of this and that, about the past grandeur of seaside cities on the Channel and, gradually, the conversation shifts to more sensitive topics, most notably Brexit, suggesting that things in the UK are not as good as they used to be. The conversation then mentions, in an easy-going way, that in Shanghai people are very nice and friendly, that if you go to a restaurant everybody will greet you and people are keen to know more about Europe. Conoscenti asks 'Who is the sender of this message?' People in the audience, mother-tongue speakers of English, answer 'The BBC, probably the World Service'. Conoscenti then reveals that 'This is a shortwave emission from China Radio International directed to Europe', and explains:

> The two people speak with a British accent and use familiar elements to frame their messages – they speak the 'language of the neighbourhood' – enacting a rather basic, old-fashioned form of propaganda but the same approach is now used at every level: social media, shortwaves, and more.

As Conoscenti explains, we can identify, in this kind of broadcast, three main phases: 1) the introduction of the topic within a familiar framing, corresponding to the engagement of the audience, 2) the gradual reframing of the topic, shifting towards a Chinese perspective on the issue, and, 3) the influence phase, where the goal of the previous two phases is made clear: China has its own, better solution to the problem.

Today, while the BBC World Service is shutting down frequencies, China Radio International (CRI) uses 552 frequencies to broadcast programmes in 61 languages. In fact, according to what CRI itself writes on its website, it has 'the most language services among all global media organizations'. The broadcaster targets, with a consistent master message, Africa, Europe, South America, and of course Asia. Yet, as it admits, its English service is:

> one of CRI's most important divisions. We provide the world with one of the most efficient and convenient ways of learning about China. We focus on news reporting as well as produce a variety of feature programs.

China's new Information Support Force, previously tied to the Strategic Support Force, is now under the control of the Central Military Commission. This change gives Xi Jinping even more direct control over the military apparatus and points to the next step in Chinese disinformation efforts. 'The result', says Conoscenti, 'is that China is developing a Kremlin-style disinformation playbook: they use massive cross-platform interference campaigns on Facebook, YouTube, TikTok, and even Pinterest' and this is part of a larger and more articulated strategy. Consider what Xi Jinping said at the 30th collective study session of the Political Bureau in 2023: China must 'construct a strategic communication system', enhance 'international communication influence', and show the 'persuasive power of Chinese discourse' as well as its 'ability to guide international public opinion'. Additionally, China must 'accelerate the construction of its discourse and narrative system' and 'strengthen the propaganda and interpretation of the Communist Party of China'. This involves 'in-depth research from various perspectives, including politics, economy, culture, society, and ecological civilization, centred on the Chinese spirit, values, and strength'.

As for Russia, in May 2023 President Putin approved a document stating that 'It is necessary to continue adjusting approaches to building relations with unfriendly states' and 'It is important to establish a mechanism for identifying vulnerable points in their foreign and domestic policies to develop practical steps to weaken

Russia's opponents'. The document emphasizes that 'Comprehensive deterrence of unfriendly countries must be carried out through offensive information campaigns', which must cover 'military-political, trade-economic, information, psychological, value, and other spheres' as well as 'new major themes in foreign policy activities' such as 'the fight against neocolonialism', the promotion of 'traditional spiritual and moral values' and support to 'states and interstate associations inclined towards constructing interaction with Russia'.

As hinted above and emphasized by Conoscenti, 'We should be aware that disinformation efforts are not limited to any single technology or digital platform. China and Russia are adopting a comprehensive 360° approach'. Our focus, therefore, should be on processes and methods, rather than on specific tools or technologies. And this is Conoscenti's main argument: 'Tools and technologies are merely the finger pointing to the moon; it is the process and the methodology that matter'. For example, in 2018 John Kelly and Camille François discovered that:

> Instead of trying to force their messages into the mainstream, these adversaries target polarized communities and 'embed' fake accounts within them. The false personas engage with real people in those communities to build credibility. Once their influence has been established, they can introduce new viewpoints and amplify divisive and inflammatory narratives that are already circulating. It's the digital equivalent of moving to an isolated and tight-knit community, *using its own language quirks and catering to its obsessions*, running for mayor, and then using that position to influence national politics. [emphasis added]

Thus, Conoscenti clarifies, from a linguistic perspective the key elements that apply across platforms are audience architecture, language engineering, the already-mentioned language of the neighbourhood, and the larger ecosystem, which is itself based on the regularities of the language. From this, it follows that:

> If we want to counter disinformation, we need to understand both the language of our opponents and our own. We need to find ways to produce a language that resonates with the narratives we want to promote. We must counter their narrative while at the same time establishing our own.

The point is that neither NATO nor the EU has a specific strategic communication strategy and they are thus followers rather than trendsetters in this important arena. Furthermore, the former does not yet have a 'NATO-agreed' definition of 'strategic communication'. Meanwhile, authoritarian regimes actively work on this important element of today's FIMI.

Shifting the focus from verbal to visual communication, **Massimiliano Fusari** discusses the role played by visual media in today's communication processes by applying storytelling techniques specifically to international politics.

'The present is visual', argues Fusari:

> as today 90%+ of all data on the internet is visual, in one form or another. Yet, communication has always been visual, and surely will continue to be so.

> Visual communication is, and has always been, key to strategize effective and impactful messages across all sectors of societies and cultures. And now, to an unparalleled level, to fight the war of perceptions, and hence of nudging the hearts and minds, of international audiences on political issues.

When thinking about international relations, consider, for example, the following picture of King Charles III at COP28 in Dubai (see ***Image 1)***.

It was King Charles' first international appearance as king, and he is wearing his formal attire, with a tie and a pochette. The imagery on these accessories, however, presents a less conventional choice, as Fusari points out:

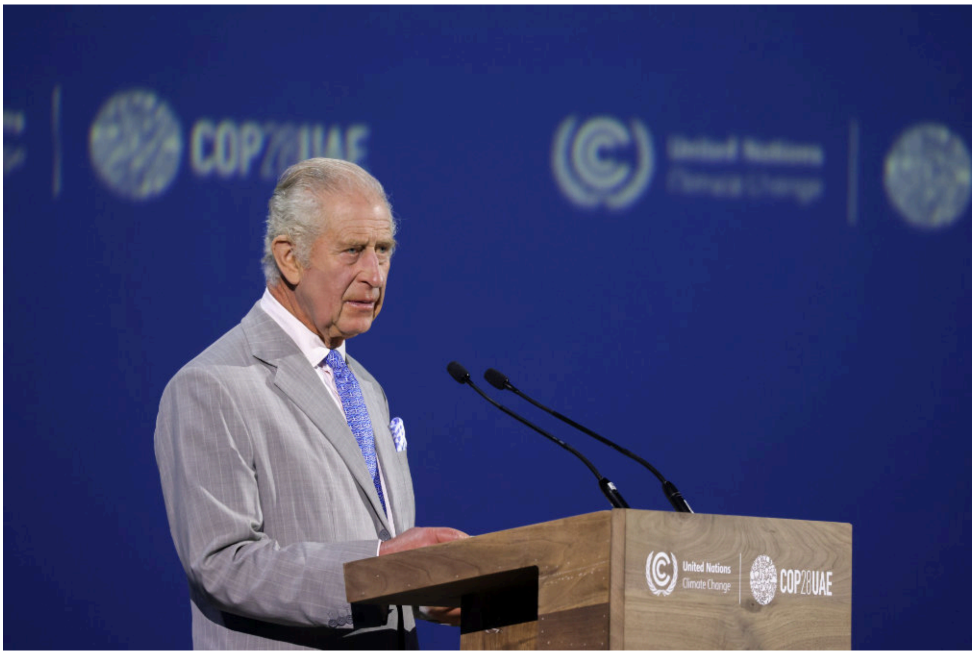
> it is a Greek flag endlessly multiplied on both accessories, which has been widely interpreted as an implicit sign of support for Greek Prime Minister Kyriakos Mitsotakis over the recent quarrel he had with his UK counterpart for the return of the Parthenon marbles from the British Museum. To deplore his PM's attitude of refusing even to meet to discuss the matter, King Charles stated his position *clearly* yet *silently*, and managed to do so without any chance of being accused of interfering with the internal affairs of his government: it was his *implicit* way to *explicitly* communicate a *strategic* message.

'Storytelling', Fusari explains, 'aims to align *projected* messages with *perceived* messages by *strategically* using the right combination of "format" and "content"'. As the example above illustrates, visuals can be a formidable storytelling device for communicating intended messages, at both personal and social levels.

Building on this insight, Fusari delves into a case study to flesh out the role of visual storytelling in international relations. The case is that of the website saturday-october-seven.com, which was devised by its author(s) to denounce the attacks perpetrated by Hamas on 7 October 2023.

Image 1
King Charles III at COP28

Source: COP28/Christophe Viseux/Flickr



Bracketing out any discussion or judgement of the events, to focus instead on the way in which the author(s) of the website have communicated their message, Fusari highlights how, already on the home page, there are some key details to focus on.

The first element that appears on the home page is a trigger warning: ‘This website contains extremely difficult to watch content from the terrible massacre carried out by Hamas on the seventh of October’ (see ***Image 2***). As Fusari explains:

> the warning is written in English, and this element leads us to speculate that the website is meant primarily for an English-speaking, and arguably international, audience. As there is no option to choose the website language, which is a rather common practice in international communication, we could easily assume that the intended policy of dissemination, either by conscious decision or language limitations, is indeed to target an English-speaking international audience.

Addressing such a (politically) heated and (emotionally) sensitive topic cannot be done without explicitly stating that this contribution does not – in any way – form any part of the discussion of the military confrontation, as it aims to discuss solely the policy of communication of one of the actors without taking sides in any way. In addition, the images of these dramatic events are here presented as public documentation that is widely available in a multiplicity of media formats, but might, still, because of their content, hurt personal and/or public sensibilities.

The website domain was registered (as per the internet provider GoDaddy) on 19 October, twelve days after the events in question. As Fusari points out:

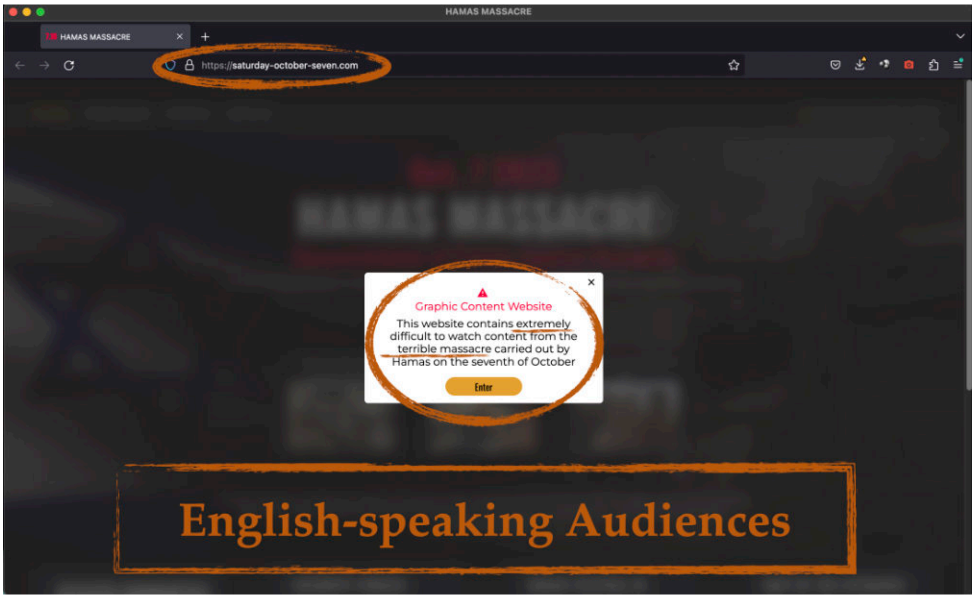
> many alternative domain names were then and are still available almost a year later, and different options could have been chosen at that time, including, for instance, ‘october-seven’. It is therefore reasonable to conclude that including ‘Saturday’, the holy day for Jews, might be intended as a conscious and explicit reminder of the un-holiness dimension of the perpetrated attack.

This consideration is indirectly reinforced by the heading ‘HAMAS MASSACRE’ being consistently repeated and capitalized across all pages and sections of the website, which, combined with the dedicated email address provided (hamasmassacre@gmail.com), ‘explicitly restates the gravity of the attack’. Finally, Fusari notes:

> all the materials on the website were uploaded on the very same day of the website purchase, with no changes since, which dramatically limits its appearance results on Google searches, as content updates are a key metric for positioning on the top of Google’s search engine.

Unsurprisingly, there are several different websites dedicated to the events that occurred on 7 October, each using different frameworks and approaches to storytelling, with varying communication strategies and dedicated supporting materials. In the case of saturday-october-seven.com, Fusari briefly addresses some basic concerns about the visual, with explicit reference to the design of the user interface (UI), or, in simpler terms, the look of the website.

Image 2
Trigger warning as users access the saturday-october-seven.com website.


HAMAS MASSACRE

https://saturday-october-seven.com

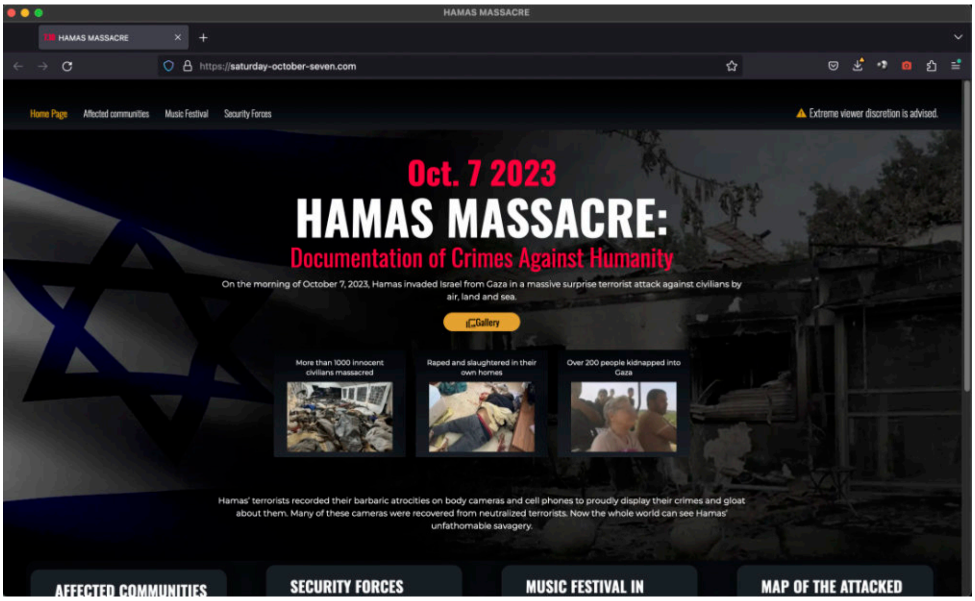
Graphic Content Website

This website contains extremely difficult to watch content from the terrible massacre carried out by Hamas on the seventh of October

Enter

English-speaking Audiences

Image 3
Homepage of the saturday-october-seven.com website


HAMAS MASSACRE

https://saturday-october-seven.com

Home Page Affected communities Music Festival Security Forces

Extreme viewer discretion is advised.

Oct. 7 2023

HAMAS MASSACRE:

Documentation of Crimes Against Humanity

On the morning of October 7, 2023, Hamas invaded Israel from Gaza in a massive surprise terrorist attack against civilians by air, land and sea.

Gallery

More than 1000 innocent civilians massacred

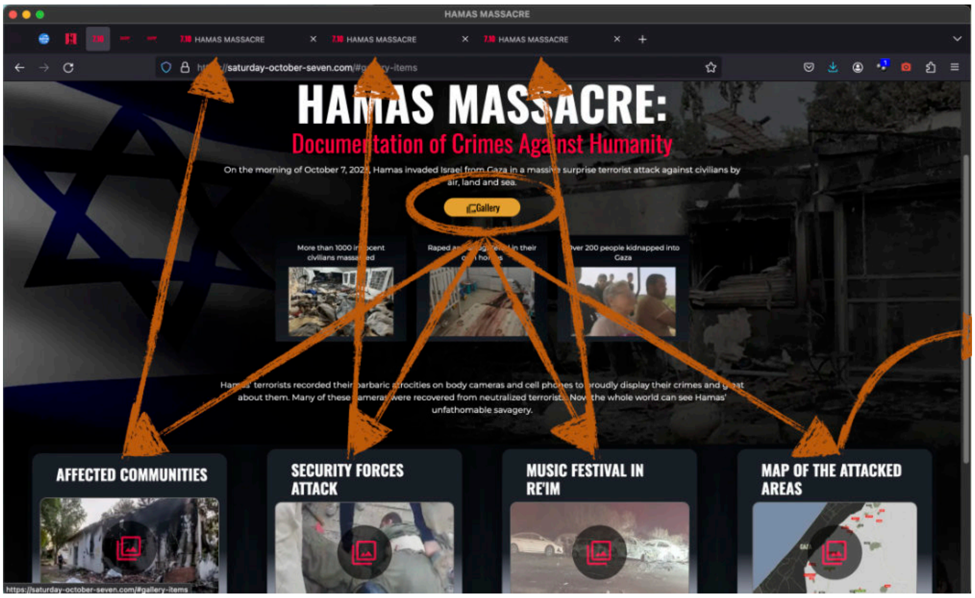
Raped and slaughtered in their own homes

Over 200 people kidnapped into Gaza

Hamas' terrorists recorded their barbaric atrocities on body cameras and cell phones to proudly display their crimes and gloat about them. Many of these cameras were recovered from neutralized terrorists. Now the whole world can see Hamas' unfathomable savagery.

AFFECTED COMMUNITIES SECURITY FORCES MUSIC FESTIVAL IN MAP OF THE ATTACKED

Image 4
Homepage and galleries of the saturday-october-seven.com website.


HAMAS MASSACRE

HAMAS MASSACRE:

Documentation of Crimes Against Humanity

Gallery

AFFECTED COMMUNITIES

SECURITY FORCES ATTACK

MUSIC FESTIVAL IN RE'IM

MAP OF THE ATTACKED AREAS

https://saturday-october-seven.com/#gallery-items

As shown in the image above, 'HAMAS MASSACRE' is at the centre of the page to explicitly state the 'mission' the website has taken on: that is, to collect 'Documentation of Crimes against Humanity' (see ***Image 3***). In the background there are two images: on the left an Israeli flag, on the right a picture that *may* show the outcome of one of the attacks. 'Arguably', Fusari comments, 'the visual connection is there to produce a [perception of] cause–effect relation with an explicitly stated agency, Hamas'. Next, between two short blurbs, a line of accusations presents a brief summary of the impact of the attack, in three points: 'More than 1000 innocent civilians massacred', 'Raped and slaughtered in their own homes', 'Over 200 people kidnapped into Gaza'. Scrolling down the page, there is a more detailed articulation of the impact of the events by reference to four thematic galleries: 'AFFECTED COMMUNITIES', 'SECURITY FORCES ATTACK', 'MUSIC FESTIVAL IN RE'IM', and 'MAP OF THE ATTACKED AREAS' (see ***Image 4***).

These galleries represent 'storytelling categories used to lead the understanding of the events' and, once they are opened, 'the same title for each section is repeated: "HAMAS MASSACRE"'. As Fusari argues, 'this feature tends to be counterproductive when aiming to maximize communication impact, as it overall limits the user experience' (UX). This, Fusari says,

> 'might be because of any of these possibilities: either the website owner(s) might wish to restate their intended accusation over and over, or, possibly, the details of the UX, as a communication policy, might have been of secondary relevance to them in comparison to the gravity of the materials shared. Finally, a third option might be that the owner(s) might not have known how to diversify the heading structure.

Moreover, as Fusari points out, there is a discrepancy in the website's UX: the first three thematic galleries are dedicated photo galleries, but the fourth – a map – is shown as an overlaid single image and is not listed in the menu at the top left. Fusari interprets these inconsistencies with the possibility that the website might not have been professionally designed. Another possible reason, he adds, is that:

> the focus of the website might have been to favour 'content' over 'form', assessing the former as strong enough to overlook the latter. Yet effective storytelling is that which produces an impact, and it delivers it by combining content with form in an intentional and finalized, and hence strategic, manner.

As Fusari argues,

> visualization is information: the form you use to show something surely impacts, and oftentimes informs, its reception. For instance, whispering or screaming (as a strategy of communication) the same message produces rather different outcomes, and yet the right form depends on a variety of factors, including whether we actually wanted that message to be heard (intentionality). Raw messages communicate too, but they are not storytelling as they are not defined by strategy or intentionality. For instance, the same scream might come out your mouth because of a hammer mis-targeting your finger as you try to fix a nail on the wall, or as an intended call for help. One is intentional, the other is not. One is part of a strategy, the other is not.

Indeed, Fusari clarifies:

> whereas anything has the potential to communicate, what explicitly differentiates storytelling from messages is its intentionality to use the 'form' component (one of the strategic aspects) to its full potential. We are aware that any unequivocal differentiation of storytelling from messages would benefit from a more articulated review. For the present context, let's agree that visual storytelling refers to a visual message which has been intentionally enhanced with an intended communication strategy that takes full advantage of the specificities of its media form.

According to Fusari, on the saturday-october-seven.com website, various storytelling techniques could have been used to shape the visual messages more thoroughly and impactfully. Yet:

> the overall impression is that images were dumped into the website without any criteria or strategy of communication. For whatever reason – rage, desperation, or simply inability, or disinterest in the form's potentiality – images are presented as 'raw content' with the implication that audiences should make sense of them by themselves. Arguably, images were perceived as 'self-sustaining' their messages (the massacre by Hamas) as truly effective communication content, without requiring any further support by 'form'.

The picture below, for example, could convey different messages by providing different captions and tags (see ***Image 5***). Per se:

> the image looks very much like a dramatic car accident that we could witness on any road everywhere. By providing verbal support in the form of a caption, or a tag, the visual content could have been better intended, and more effectively communicated.

Indeed, to reiterate the point raised above, raw messages are part of communication and surely communicate. Yet, images seldom, if ever, have an *objective* value in and of themselves: their meaning is contextualized. 'One tactic of contextualization', Fusari continues:

> is indeed verbal support, in the form of a caption or a tag. Yet there is another tactic that might be even more impactful because it works in an implicit, rather than explicit (like a caption), manner, and this is sequencing images strategically.

For example, when accessing one of the thematic galleries on the saturday-october-seven.com website, the user is exposed to a wall of distressing images with no detectable order:

> How would, or could, or indeed should the user read and make sense of these images? What is their starting point? What is their line of development? How does their number and grid of presentation influence the user's ability to read, understand, and finally appreciate their intended communication?

Image 5
One of the images featured in the saturday-october-seven.com website.

In asking this, Fusari stresses once again that ‘form’ is ‘content’: ‘the former without the latter underperforms its duties – and this is why storytelling should be conceived as the strategic combination of the two (content with form) to produce an impact.’ Indeed, in the case of the saturday-october-seven.com website:

> by strategically ordering visual content and providing a revealing index to such order, the author(s) of the website could have led audiences to make sense of the presented materials in a way – hopefully – as close as possible to the way that was intended. Or, said otherwise, purposeful and strategic editing can help align projection with perception.

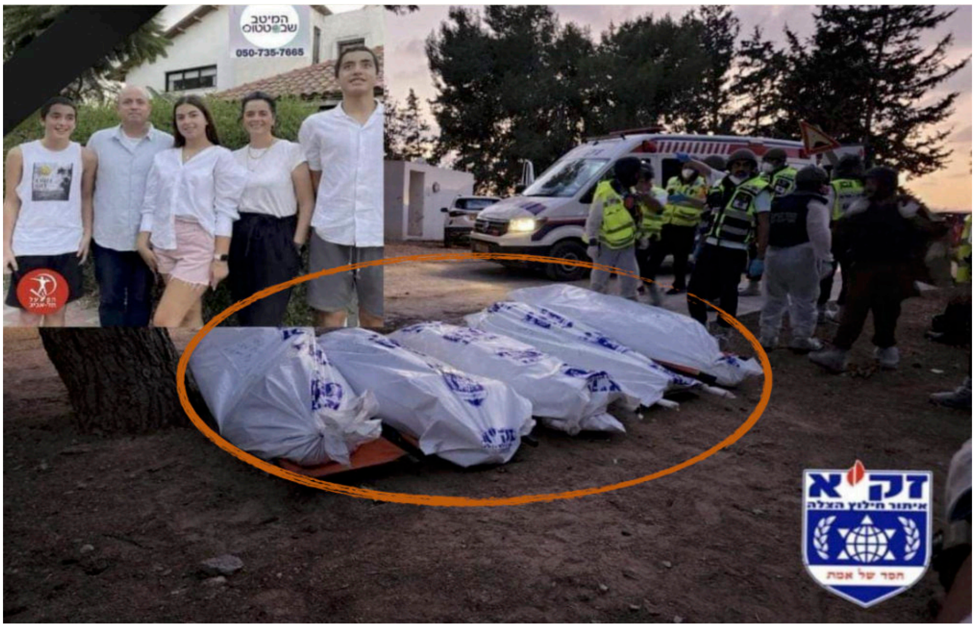
For example, Fusari goes on to explain:

> combining the two images below [see ***Image 6***] in the same frame strategically highlighted the before-and-after of the events of 7 October, capturing the cruelty and horror of the attacks by leading to an implicit identification of the five dead bodies in the bags as the five smiling people on the top left, and, eventually, as a family, which would add another layer of impactful emotions.

Importantly, all the above considerations merely scratch the surface of the extremely rich possibilities for communication that visual media offer: ‘By its own nature, visual communication endlessly articulates multiple and coexistent messages that visual storytelling fights to manage and articulate with intentionality by strategically engaging the form component.’ Eventually, Fusari admits:

> my line of reasoning might prove to be nothing more than mere speculations, as whatever I might have seen (and hence interpreted) in those images and the website structure might actually prove to be nothing more than my own analytical journey of interpretations. After all, this is not so uncommon, precisely because of the dramatic volatility of *visual* meaning-making processes and the complexities of the human being.

Image 6
A combination of two images featured in the saturday-october-seven.com website



In such a context, Fusari's explicit aim is to warn of the intricacies of the relations among the sender(s) and the receiver(s) of either intended or unintended messages because of the virtually infinite possibilities of interpretation(s) and reading(s) of the same communication materials. Fusari closes by adding that:

> these complexities must be acknowledged and critically addressed, as even being aware of these dynamics, in itself, already represents already a basic level of visual competency, which remains key to today's communication processes, whatever its formats. Unfortunately, when looking at images, nothing is ever for sure. Hence, visual storytelling is that set of dedicated tools required to channel the multifaceted explosions of meanings that images produce as messages by using intentionality and strategy to make projected messages one with perceived ones.

Following through with a more institutional focus, **Matthew Heneghan** sheds light on processes and patterns of disinformation in Central Asia between the geopolitical shocks of the COVID-19 pandemic and the onset of Russia's full-scale war against Ukraine. He begins by emphasizing the importance of recognizing that the diffusion of norms and ideas concerning disinformation, and how it should be addressed by governments, varies significantly outside the transatlantic region.

Central Asia is one of the most rapidly growing regions in terms of internet penetration and digitalization strategies, which are primarily driven by state actors with marginal input from the private sector. In the five Central Asian states – Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, and Uzbekistan – up to 95% of daily internet traffic passes through Russian servers, while Russian state media broadcast across the region as per intergovernmental agreements stemming from the Commonwealth of Independent States (CIS) era in the 1990s. Local media outlets across Central Asia, though they are not under the direct jurisdiction of Russia's regulatory bodies, have experienced pressure from Russian state regulatory bodies to sanitize and even censor materials they broadcast. The influence of Russian state media on information consumption practices in the region, however, varies, ranging from extensive – as in Kyrgyzstan and Turkmenistan, where households regularly watch Russian state news – to less pervasive – as in Kazakhstan and Uzbekistan, where media content produced in local languages is thriving. Despite this, the development of media environments in local languages is limited and shaped by increasing restrictions, as will be discussed below.

Heneghan says:

> In order to understand what the political economy of information looked like in Central Asia at the onset of the war in 2022, it is necessary to look back to the immediate antecedent: the COVID-19 pandemic. This is when states began consolidating different strategies of information control.

The responses to COVID-19 varied significantly across states. For example, Turkmenistan completely denied the existence of COVID-19, which entailed the silencing of healthcare personnel. Meanwhile, Kazakhstan undertook total containment of the spread of the virus, which enabled the curtailing of media freedom under the remit of quarantine measures. In terms of disinformation, the information control context of the pandemic led to a unique regional phenomenon – what Heneghan describes as the 'bifurcation of disinformation categorization'. As he explains, this bifurcation entails a situation in which 'conventional fake news and conspiracy theories were conflated with and identified alongside anything that contradicted official government accounts of infection containment'. This period saw the emergence of an information infrastructure that allowed political elites to selectively frame state responses to the pandemic and, more broadly, to demonstrate their capacity to manage informational integrity domestically. Said otherwise, pandemic reporting became a mechanism for maintaining incumbent legitimacy or subduing infighting among political executives.

> It is indeed in the overlapping period between the outbreak of the pandemic and the onset of war that we observed interesting developments in the information control domain, with new laws and regulations being appended to existing legislation, often incorporating the term 'disinformation'.

For example, Kyrgyzstan's False Information Law (2020) and Uzbekistan's law against insulting political elites (2021) expanded extant defamation legislations, enabling the blocking or erasure of information online without any court order – 'de facto allowing the Kyrgyz and Uzbek governments to remove any online content they disagree with'. Along similar lines and around the same time, Kazakhstan and Kyrgyzstan expanded their 'anti-foreign-agent' measures, modelling them on Russian law: foreign service providers were required to register locally and/or localize data storage facilities, enabling snap restrictions on citizen activity and effectively allowing the government to shut down the operations of any organization receiving foreign funding – 'except for those linked to Russia', Heneghan points out, 'because Russia is not the target of such laws on curbing domestic influence'. Moreover, from 2021 onwards, all states have regularly implemented partial or full internet shutdowns in response to social unrest. The most severe instance occurred in 2022, when Kazakhstan experienced a week-long internet blockage costing the national economy more than $410 million per day and underscoring the lengths to which states can go to control information flows.

Against this backdrop, the onset of war brought about what Heneghan identifies as 'deliberative disinformation'. He explains:

> The response to the Russian invasion of Ukraine varied across Central Asian states: Kazakhstan and Uzbekistan adopted a stance of 'strategic neutrality' while Tajikistan and Turkmenistan remained silent. Yet no state recognized the invasion as outright war. They all complied with Russian regulations by using the term 'special operation'.

This period saw further bifurcation of disinformation and inconsistent state approaches. On the one hand, Central Asian states echoed Russian grand narratives concerning the justification of war (e.g. anti-NATO sentiments and accusations of repression of ethnic Russians in the east of Ukraine). At the same time, however, they selectively published information about the actualities of the conflict in Ukraine, such as the massacre in Bucha. It is at this point that disinformation became a deliberative process, requiring the triangulation of different regulatory frameworks from the Russian side, executive politics from domestic actors, Western development conditionality (which made it impossible for Central Asian states to adopt a totally pro-Russia/anti-Ukraine stance), and civilian pressures and counter-narratives. According to Heneghan, this process also led to an adjacency and spillover effect of war reporting, whereby coverage of war atrocities made the contours of independent media and civil society more visible, prompting states to further constrain non-governmental support for combating dis/misinformation.

In order to understand these complex regional dynamics, Heneghan proposes the concept of 'regime coherentism': a framework in which to understand regional consensus-building in relation to information management in Central Asia. As Heneghan explains, since the 1990s all Central Asian states have been seeking (collective) ideational security and survival through inter-regional institutions such as the CIS, the Collective Security Treaty Organization (CSTO), and most recently the Eurasian Economic Union (EAEU). These institutions deepen cooperation and structural dependency vis-à-vis Russia, and are mutually reinforcing in terms of regime survival. Said otherwise, in Central Asia regionalization represents an ontological security act – and therefore 'Russian narratives to justify the war in Ukraine cannot be deemed illegitimate or criticized as doing so could threaten the very political and institutional arrangements between Central Asian states'. Rather, 'Central Asian states need to engage in strategically ambiguous and concurrent subscription to different "truth regimes"' and thus both deliberative disinformation and the issue of discerning the integrity of any informational unit in the region depend on 'the momentary positionalities and levels of structural dependency of state regimes vis-à-vis Russia, the EU, the US, and large private-sector actors'.

According to Heneghan, 'it is therefore important to acknowledge that disinformation in Central Asia can be damaging for domestic and/or international relations while also enhancing regime support, capacity, and survival'. Attempting to navigate this paradox by providing funds to digital civil society and independent media will hardly be enough. ‘In order to counter disinformation in authoritarian settings’, says Heneghan, ‘there is a need to incentivize state-level cooperation to break away from the regime coherence effect’. Heneghan suggests three ways to do so. One avenue is pushing for a regional, mutually brokered, legal definition of ‘disinformation’ that robustly distinguishes between harmful information and free expression online, thereby preventing the misuse of disinformation laws to stifle dissent. Supporting the development of local-language digital media to achieve equivalence with Russian-language sources is also crucial. Likewise, a bolstered focus on English-language education would help to circumvent the Kremlin’s influence and build media literacy across Central Asia, although the long-term goal should be to build a strong native media environment. Finally, ‘we can approach digital development programming as a means to build societal and institutional capacity without an explicit emphasis on regime politics or controversial topics such as the ongoing war in Ukraine’. Yet, Heneghan concludes, we are thus faced with an ethical dilemma as to whether it would be right to pursue such a ‘sanitized’ development agenda ‘without transparency about donor positions and aims’.

PANEL 2

Addressing authoritarianism in digital governance

On 20 September 1987, the very first email was sent from China, declaring with high hopes that 'Across the Great Wall we can reach every corner in the world'. More than 35 years later, however, what is now known as the Great (Fire)Wall of China has created a world unto itself, whereby 'those inside the Firewall cannot see outside, and those outside cannot see inside' says **Fang-Long Shih**, the first speaker of the second panel. Nevertheless, a crucial exception is how the Chinese government itself transcends that Firewall to engage in increasingly sophisticated and pervasive forms of illicit internet activity beyond the national boundaries of the Firewall.

In fact, Shih recounts:

> while in the 1990s the Chinese government vocally supported the expansion of internet connectivity, it simultaneously took steps to control it as soon as the internet was opened to the general public in 1995. And in 1997, the Chinese Ministry of Public Security issued the Measures for Security Protection Administration of the International Networking of Computer Information Networks, which were approved by the State Council. In the same year, Beijing introduced its first laws criminalizing online postings considered to represent a threat to national security, which pragmatically means the security of the Chinese Communist Party (CCP).

Indeed, as DigiChina specialist Rogier Creemers observed in 2017, 'As the internet became a publicly accessible information and communication platform, there was no debate about whether it should fall under government supervision, only about how such control would be implemented in practice'. Said otherwise, Shih observes that:

> organizational warfare (*zuzhi zhan*, 組織戰) played a significant role in the CCP's initial consolidation of power. 'Mobilizing one group of people to fight against another (*qunzhong dou qunzhong*, 群眾鬥群眾)' has, since the CCP's rise, become an iconic tactic in cracking down on enemies and dissidents.

Shih further comments that, since the advent of the digital age, 'controlling the internet has always been part and parcel of China's digital governance, which is central to maintaining the CCP's hold on power'.

Shih's presentation is thus not about how the digital world could change China, but how China has changed the digital world. The Great Firewall is a sophisticated system of techniques and methods that the Chinese government uses to balance internet connectivity with tight controls. One of the most pervasive ways in which the Great Firewall is used to censor online content is called 'sniffing'. This refers to how the CCP deploys intrusion detection technologies to detect and block keywords that are deemed sensitive by the government (examples include the terms 'Xi Jinping', 'Taiwan independence', 'democracy').

The Firewall works in conjunction with behaviour-based methods, whereby censors analyse web traffic and server names to find suspicious websites and block them manually. Certain domains – such as google.com or facebook.com – are blacklisted, meaning Chinese users are unable to access them without bypassing the ever-tighter meshes of the Great Firewall. For example, Shih notes, 'In the 1990s, any of China's internet forums known as BBS (Bulletin Board Systems) having more than 1,000 views could attract police attention. Later, in the Weibo era, the threshold has halved to 500'. At the same time, websites and apps that wish to operate in China need an Internet Content Provider (ICP) registration permit issued by the Chinese government.

It is important to note, however, that such censorship functions are not performed purely by government agencies. Indeed, to control the digital world, the Chinese government often outsources censorship to domestic and international companies – such as the US-based Cisco Systems, which helped the CCP build the Great Firewall. By using market mechanisms and fostering competition within the private sector, the Chinese government ensures that its censorship efforts remain efficient and updated. As Shih further explains:

> Domestic private companies often compete for government contracts, striving to be as effective as possible due to small profit margins. If these efforts were carried out solely by government agencies and civil servants, they would likely be less efficient due to a lack of profit motive and market competition.

China's digital governance is therefore not characterized by complete control. Rather, as hinted above, the CCP has engaged in a careful and delicate balancing act between connectivity and control, devolving some key parameters of control to the private sector. Thus, the CCP's authoritarian control is not directly administered. Nor is its authoritarian control absolute since, as Shih emphasizes:

> Chinese netizens and dissidents have found creative ways to elude the filtering and blocking of online content. For instance, some netizens are adept at using sarcasm, as in the case of the hashtag *#ChinaIsAGreatPlaceToLive*, or the many mocking posts shared online during the COVID-19 pandemic, such as '*We need to refuse the vaccine in the horrible West, because chief Hu's [Hu Xijin, of the Global Times state media] saliva drops are the best vaccines for us*'.

Some Chinese dissidents are also able to bypass the Great Firewall through quasi-legal virtual private networks (VPNs), 'but most who use VPNs do so for purposes not seen as threatening by the CCP, and hence implicitly condoned', clarifies Shih. The point, she continues, is that 'the CCP always reserves the potential to clamp down in particular circumstances (such as on 4 June [the date of the Tiananmen Square protests] and 1 October [National Day] or during the People's Congress period) or in relation to the proliferation of certain searches or trigger words. According to one of Shih's informants, 'If I really want to circumvent the extant barrier, it is becoming more and more time-consuming, at times up to 40 minutes for a single search'. Other informants say that despite the opportunities that do exist for many to overcome the Firewall, 'most Chinese citizens do not bother because they are happy to operate within the Firewall and they deem the information they could access beyond the Firewall "not of use" for them in China'.

Shih concludes that in the information age, the strategy of organizational warfare has become even more intensified. The CCP uses the Firewall to continue mobilizing one group of people inside the Firewall (known as *Xiaofenhong*, 小粉紅) to fight against another group outside the Firewall. These dynamics inside and outside the Firewall lead to social division within China and between China and the rest of the world. This aligns with Mao Zedong's saying 'greater chaos in the world, greater benefits [to the CCP] (天下大亂，形勢大好)', which later became a guiding principle of the CCP. The CCP builds up and mobilizes any perceived threat to social cohesion for its own benefits, 'using it as justification for its surveillance, censorship, and crackdown on so-called "dissidents", whether they are located within the Firewall or in countries beyond it'. These digital trends allow for an increasing range of ways to stabilize Chinese authoritarian governance and allow rules, norms, and algorithms to be manipulated so that citizens are cajoled into acting out the leadership's will. The Chinese government's control has developed a logic of its own, epitomized by the omni-surveillant reach of the social credit system (社會信用體系). The CCP has taken key elements of digital technology in a new authoritarian direction, primarily geared to preventing opposition and dissent. This raises the question of whether China's deployment of digital technology should be seen in a comparative and historical perspective as exceptional – as a substantial change – or merely as a change in intensity.

Reflecting on the rise of digital authoritarianism as a general phenomenon, **Giampiero Giacomello** recalls the optimism spurred by the advent of the internet in the mid-1990s and early 2000s:

> At the time, there was an idealistic vision that this new technology would foster global communication, support democracies, and fight autocracies. This was the focus of my PhD dissertation over 25 years ago, where I explored why governments would want to control the internet.

Back then, the internet was largely perceived as a liberating technology, while today it seems that government control has the upper hand in cyberspace. The dynamic interactions between governments, the private sector, and individual users in this domain are complex, but, as Giacomello acknowledges, it is clear that:

> unfortunately, users have lost a lot, especially in countries like China, Iran, and Russia, where governments have become very effective at controlling the internet. While this control is not absolute – because it is not absolute – it is significantly stronger than it was 30 years ago.

The rise of AI brings new considerations. AI introduces a number of security issues concerning the loss of privacy and misuse of personal data, of course, but it also interacts with cyberspace in intriguing ways. Indeed, the two are closely connected, not least because computational models unravel in cyberspace. Thus, gaining a better understanding of contemporary issues in cyberspace cannot be separated from shedding light on how great powers cope with AI.

AI depends on machine learning and therefore needs a massive volume of high-quality data to train large language models. As Giacomello says, 'Nowadays, high-quality data are like the gold standard. They are like oil'. In this domain, the entrepreneurial abilities and resources of the US obviously stand out. Yet, Giacomello argues, the US does not represent the most interesting actor to focus on, despite its leadership position. Rather, Giacomello often wonders about China's approach to AI:

> Large language models need to conform to practice guidelines. They cannot deviate from them. How does China train models under such constraints? Some machine-learning experts suggest that China wants us to believe they are limited by these rules, while in fact their explorations are likely to be further ahead than we think, possibly on par with or even surpassing those of the United States. But even if that were the case, key questions remain: what kind of data is China using? As mentioned, training large language models requires a huge amount of data. These data are often sourced from the internet and are predominantly in English. Does China train Chinese models with English texts?

On the other hand, Russia has tremendous brainpower but lacks material resources for AI. 'Russians are following their own path, but are not major competitors in this field', says Giacomello. Instead, he adds, 'Saudi Arabia and the United Arab Emirates are investing heavily in AI and are emerging as potential competitors, raising questions about their own approach to AI given that these countries are not known for their democratic attitudes either'.

Europe, for its part, has a peculiar approach to technology: there are no significant European champions in the technology race and Europe, as a whole, seems to be operating in the American arena. At the same time, the EU seems content to serve as a regulator, as evidenced by the success of the General Data Protection Regulation (GDPR) in influencing global practices – even though, as Giacomello points out, it remains uncertain whether this regulatory success will extend to AI. All in all, it seems that 'the European Union has resigned itself to being a regulatory and cultural power rather than a competitive force in technology. It seems that Europe has given up on competing with the United States or China in this arena'.

These dynamics bring us back to Giacomello's initial reflections on the history of the internet or, rather, to the zeitgeist – the spirit of the time in which the internet first emerged, and also that of the one in which AI is now unravelling. Giacomello explains:

> Technology is neutral but it is highly influenced by the broader global environment. When the internet became widely available, there were high hopes and positive attitudes. With the end of the Cold War, many countries were embracing democracy, and it seemed the world was changing for the better. Technologies and optimism influenced each other, creating a sense of progress. Fast forward to today, we find ourselves back to great power competition and AI is seen as a tool for increasing control and machines as potentially dominating humans.

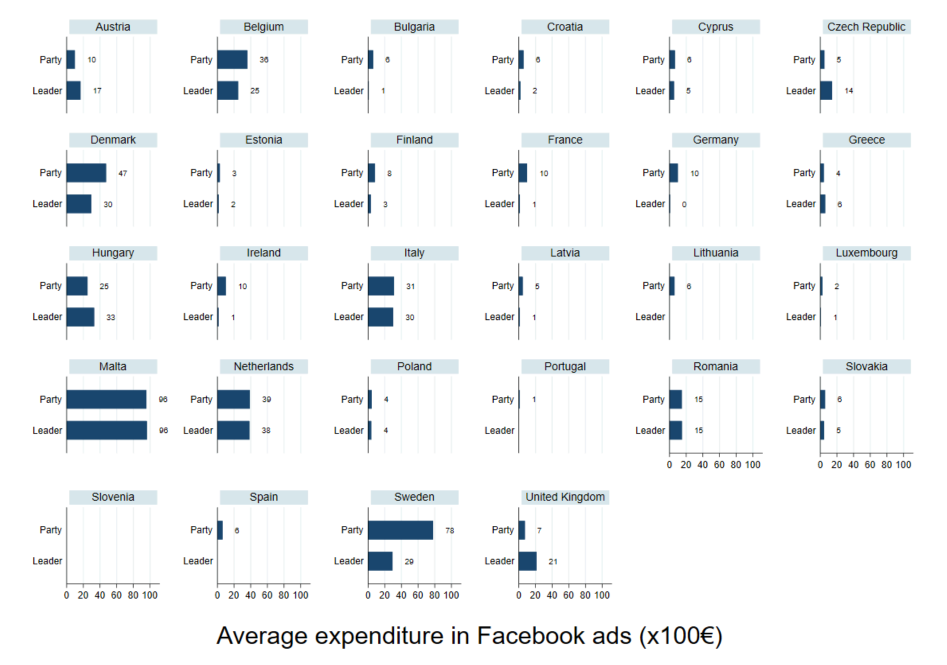
Said otherwise, it is challenging to separate the influence of contextual factors from the real and perceived impacts of technology itself, as the two deeply affect each other. The relationship between politics and technology remains a fundamental force of our societies. Yet 'our attitudes and perceptions have reversed, now highlighting the potential for these technologies to be used for control rather than liberation'.

Taking their lead from Giacomello's insight on the European stance in digital governance, **Antonella Seddone** and **Enea Fiore** discuss the role of the EU in regulating political advertising on social media, sharing some of the preliminary findings of research they are conducting with **Daniela Romée Piccio**.

Digital tools have reshaped political communication and altered the relationship between citizens and politics, contributing to the personalization of politics and the resulting marginalization of the role of political parties (i.e. disintermediation). According to Seddone, an explanation for this can be found in the operational mechanisms of digital platforms themselves: 'Digital platforms promote the dissemination of biased and misleading information, solidifying viewpoints and contributing to polarization. Algorithms prioritize content that aligns with users' existing beliefs and prejudices, reinforcing biases and creating echo chambers'. Moreover, Seddone continues, 'digital platforms collect data on opinions, attitudes, and beliefs, allowing political actors to craft their communication in highly effective and persuasive ways. These data enable political microtargeting, reaching specific population segments with tailored messages'. Thus, compared to traditional media such as television and radio, digital platforms offer a cost-effective method for targeted political marketing, making it an accessible strategy for a wider range of actors.

To gain a clearer picture of the phenomenon, Seddone and her colleagues at CODER analysed data on the expenses incurred in 2022 by the five most-voted-for parties and their leaders in the 27 EU countries and in the UK, for advertisements on Facebook and Instagram. The data showed that some countries – such as Denmark, Hungary, Italy, and Sweden – exhibited high expenditure levels (see ***Graph 1***).

To better understand these patterns, Seddone and colleagues conducted an exploratory analysis using a multilevel regression model considering both country-



Graph 1
Average expenditure in Facebook ads

Source: Antonella Seddone et al.

level and party-specific factors. 'What our findings seem to indicate', Seddone says, 'is that two variables drive greater expenditure on online political advertisement: right-wing positioning and populism' (see ***Graph 2***).

Graph 2
Variables included in multilevel regression model.

Source: Antonella Seddone et al.

	AVERAGE EXPENDITURE ON ADS PER WEEK (€)
Party Leader account	-0.730 (-0.13)
ElecBon campaign's week	-4.221 (-0.11)
Party in government posiBon	11.56 (1.03)
Ideological positioning (0:leftwing; 10:rightwing)	**3.244*** (2.37)
People centrism	**8.925*** (2.42)
Expenditure limits on Ads	-26.21 (-1.24)
Limits on tradiBonal Ads	10.19 (0.52)
RegulaBon on old media access	12.66 (0.72)
_cons	-43.75 (-1.80)
Ins1_1_1	
_cons	3.108*** (12.55)
Insig_e	
_cons	4.156*** (163.25)
N	788

Not surprisingly, the use of social media for political purposes has increasingly come under the spotlight, and the potential negative impacts of such practices have been widely debated in academia and among experts. Yet 'this issue is not merely a scholarly concern', Seddone makes clear: 'it is a pressing concern for citizens, who are calling for institutional measures to address the perceived threats to democratic processes and keep order in what could be defined a "Wild West".' Indeed, Eurobarometer data released in December 2023 reveal that European citizens are concerned about the impact that online advertising may have on the integrity of elections. When asked about the most important elements that define a free and fair electoral campaign, approximately a third of respondents expressed a desire to know who finances political advertising and sponsored content and to be able to distinguish between sponsored and non-paid content. Additionally, 27% of the respondents pointed to the need for candidates and political parties to be transparent about their targeting techniques for political advertising (see ***Graph 3***). Nevertheless, only a few EU countries currently have regulations on online advertising, and the existing measures focus solely on spending, without any provision for transparency or content. 'This highlights the need for broader and more comprehensive regulation by the EU', Seddone concludes.

In fact, the implications of online political advertising for European electoral integrity have prompted the EU to take several steps to address information manipulation, to protect citizens' privacy and to prevent external and internal agents from subverting the democratic process (e.g. foreign interference, computational propaganda, disinformation, and hate speech). As Fiore recounts, 'The first attempt at regulation was the 2018 Code of Practice on Disinformation, which aimed at ensuring greater transparency and accountability on the part of online platforms. However, its implementation was left to the platforms themselves'. The EU reinforced this Code of Practice in 2021 and again in 2022; however, 'It was only in February 2024 that the EU introduced a comprehensive regulation, moving towards a mild form of digital governance'. These legal steps address some of the main concerns of European citizens when it comes to countering information manipulation and preserving electoral integrity: service providers are required to label political advertisements, and disclose information about sponsors' identities, spending, and the specific elections that political ads are linked to. They must also keep track of advertising campaigns, establish a repository of ads directed at European citizens, and make relevant data available and accessible to interested entities (including researchers). Additionally, under the purview of the new regulation, targeting techniques that involve the processing of personal data are only permitted when explicit consent is provided, and third countries are prohibited from sponsoring political advertisements in the EU in the three months before an election or referendum.

	Debates and campaigns avoid hate speech, manipulation and lies	Voters know who finances political advertising and sponsored content and can distinguish between sponsored content and non-paid for political information	Candidates and political parties are transparent in their use of targeting techniques for political advertising
AT	54	33	26
BE	36	28	31
BG	44	42	30
CY	45	37	28
CZ	36	31	21
DE	48	30	27
DK	50	38	25
EE	57	38	20
EL	47	38	27
ES	55	36	40
FI	49	41	19
FR	39	29	26
HR	42	44	25
HU	61	31	26
IE	35	43	32
IT	42	31	21
LT	36	43	29
LU	44	38	25
LV	40	44	23
MT	56	36	39
NL	39	29	25
PL	64	29	23
PT	37	28	33
RO	35	35	37
SE	55	38	18
SI	47	43	15
SK	41	37	21
EU27	***46***	***32***	***27***

Graph 3
Eurobarometer survey: In your view, what are the most important elements that define a free and fair electoral campaign?

Source: Flash Eurobarometer 522 (Dec. 2023)

While this move from states' self-governance to an EU-wide approach is to be welcomed, 'there are some limitations', Fiore acknowledges. For instance:

> some could argue that prohibiting sponsorship only three months before an election is insufficient, as shaping public opinion is a mid- to long-term process. There are also practical challenges: social media platforms often fail to disclose detailed information or provide data in aggregate form, which hampers scientific research. Importantly, many issues, such as polarization and hate speech, remain largely unaddressed.

Disinformation remains a challenge, within and beyond Europe. Indeed:

> if we overcame our Eurocentric tendencies, we would realize that, contrary to popular belief, authoritarian actors are more actively involved in the proliferation of manipulated content *outside* of Europe – demonstrating the lack of shared international tools to tackle the sources of disinformation and authoritarian digital practices and highlighting the need for global cooperation beyond Europe's borders or legal frameworks.

PANEL 3

Our shared digital future: recommendations for public-private cooperation

Starting off the third panel, **Kenddrick Chan** outlines some of the tenets underpinning the ways in which the private sector engages with governments in digital governance.

Today there is little doubt that governing the digital domain requires the involvement of the private sector, and Chan identifies at least five reasons why this is so. First, the private sector is the driving force behind digital innovation and is responsible for the development of the very technologies being discussed by governments and multilateral organizations. Second, and relatedly, the digital domain is not just a possible source of disruption but also an extremely potent amplifier. As Chan explains, 'during the Cold War an *agent provocateur* could influence a crowd, but in the digital age – and thanks to the technologies that private companies are responsible for – this effect is exponentially greater, reaching global audiences across digital platforms'. Third, private companies provide essential financial and communication services to their customers, thereby occupying an important and trusted role in society. Fourth, they have demonstrated their willingness to take on more responsibility, as in the case of private-sector-led initiatives such as the Cybersecurity Tech Accord or Microsoft's 'Digital Geneva Convention' – 'whether these initiatives have achieved or can achieve their goals is debatable, but the commitment of the private sector is clear', Chan comments. Lastly, governments need 'the technical expertise of private companies to ensure compliance with any policy passed'. All this, Chan ponders, 'makes private companies a valuable partner to governments; but a crucial question remains: are private companies and governments equal partners in digital governance? Can they ever be equal partners?'.

According to Chan, governments cooperate with the private sector in three broad areas, namely policy formulation, policy implementation, and technical development. As for policy formulation, Chan says:

> whereas many people assume that governments have a monopoly on setting national strategies, at the highest level governments often rely on tech companies to steer the national direction on digital policy. For example, the AI Safety Board of the US Homeland Security includes members from OpenAI, Nvidia, Microsoft, and Google.

Likewise, despite all the discussions on 'digital sovereignty', 'we need to realize that even advanced countries' governments often enter into commercial contracts with private companies as the latter are often more agile and efficient than most state-backed tech agencies'. When it comes to policy implementation, governments rely heavily on the private sector to provide them with the information needed to act effectively – 'you cannot regulate what you cannot measure'. Moreover, governments need 'data on the reach and impact of news or fake news, which only private companies can provide. In return, private companies need reassurance and "signals" regarding governments' plans'. Private companies also allow for a greater degree of agility in regulation:

> as the case of the blanket internet shutdown in Kazakhstan mentioned by Heneghan demonstrates, it is becoming quite clear that these kinds of restrictive approaches are very costly and risky. Today most governments

> prefer a conditionally restrictive rather than wholly prohibitive regulatory approach to their ecosystems – hence the private sector is seen as a partner.

Most obviously, and as hinted above, the private sector is a key partner when it comes to technical development: on the one hand, private–public cooperation allows for the combining of resources and the facilitation of large-scale investments, as well as resource and talent access that neither could achieve alone. On the other hand, the private sector relies on governments to create a national ecosystem conducive to businesses, while governments rely on the private sector to create a national ecosystem that fosters innovation and provides employment. Additionally, Chan points out that an often-overlooked area of cooperation is global governance: 'the complexity and reach of transnational issues require the buy-in of the private sector for effective management'. Countering disinformation is a case in point, as Chan explains:

> we tend to think of public–private cooperation in terms of governments working with private companies to take down content. However, changing techniques in disinformation necessitate new modes of cooperation. In an article I wrote with Mariah Thornton from LSE IDEAS, we explored a Chinese disinformation campaign targeting Taiwan and we noticed that whereas in the past disinformation campaigns relied on a single platform, like Twitter, to broadcast content, the new model uses multiple platforms, such as YouTube for hosting videos and Reddit for distributing content. If in the past governments could easily collaborate with Twitter to take down a disinformation campaign, now removing a video from YouTube would not be enough as other parts of the chain would remain intact. This shows the importance of linking efforts across platforms. Disinformation techniques are constantly evolving, and our strategies for public–private cooperation must evolve accordingly.

Public–private cooperation unfolds in multiple ways and Chan identifies four mechanisms through which the private sector engages with the public sector. First, through joint task forces and advisory boards, representatives from both sectors are brought together to provide expert guidance and strategic direction to address issues of mutual concern or interest, as in the already-mentioned case of the AI Safety Board of the US Homeland Security. Second, private companies and governments can jointly run regulatory sandboxes – that is, controlled environments where innovative companies can test new products, services, or business models under different sets of regulations, enabling mutual shaping of future policies (e.g. sandboxes by Singapore government agencies). Third, private companies and governments engage in consultations and communities of practice where networks of professionals share knowledge regarding specific areas of digital technology and provide feedback on policy proposals (e.g. the European Commission's 2022 Strengthened Code of Practice on Disinformation). Fourth, public–private cooperation often entails mutual technology transfer, whereby private-sector solutions are used to bolster the delivery of public services (e.g. use of AI and biometrics by governments for surveillance) and public-sector innovations provide massive economic benefits due to their potential for commercialization (e.g. GPS systems, the internet).

In this context, as Chan emphasizes at the beginning of his speech, one major challenge is understanding whether private companies can indeed be equal partners when it comes to global digital governance. As Chan clarifies:

> An initiative like the Cybersecurity Tech Accord clearly demonstrates the commitment of over a hundred private companies. Yet their involvement can be limited. For instance, while private companies are involved in the UN Internet Governance Forum, in July 2022 a major UN member state blocked their participation at the UN General Assembly citing their lack of sovereignty as a reason for exclusion. So private companies are not afforded full status, and this aspect calls for further discussion.

Delving deeper into one of the aspects of public–private cooperation touched on by Chan, **Tin Hinane El-Kadi** focuses on China's new 'Digital Silk Road', discussing whether it is contributing to technology transfer in the Global South.

Indeed, if over 2,200 years ago the Silk Road facilitated the global diffusion of Chinese inventions and technologies, today Chinese tech firms have made significant inroads into the digital ecosystems of several developing countries. Yet, as El-Kadi explains, 'it is not clear what the presence of Chinese ICT [information and communication technology] corporations actually means for development in the middle-income countries that are receiving Chinese digital capital'.

In 2017, Xi Jinping famously stated that big data would be integrated into the Belt and Road Initiative (BRI) to create the 'Digital Silk Road of the 21st century'. Put simply, the 'Digital Silk Road' is an umbrella term encompassing all digital projects by Chinese ICT corporations. Broadly it has three main components: *digital infrastructure* (led by firms such as Huawei and ZTE and including fibre-optic cables, network infrastructure, and data centres), *e-commerce* (with firms such as Alibaba, Tencent, and JD making significant inroads, especially in Southeast Asia), and *smart cities* (with surveillance companies such as Hikvision, Huawei, and Alibaba involved in building smart cities in developing countries through high-level contracts).

The dominant debate on the Digital Silk Road focuses on the idea that China is using network infrastructure in developing countries for espionage and that two distinct and contrasting modes of internet governance are shaping up: the Chinese model of 'internet sovereignty' or 'digital authoritarianism' versus the American model of 'internet freedom'. However, El-Kadi argues, a major problem in this debate is the portrayal of China as a monolithic actor, a result of which is that the potential conflicts between private Chinese digital firms and the state are overlooked. Moreover, there is a misconception that China has a hegemonic plan to impose its internet governance model on all developing countries. According to El-Kadi, this view neglects the fact that so far we do not have much empirical evidence about China's ability to impose its model and, more importantly, 'it neglects the fact that China's presence in many developing countries is actually demand-driven and thus mainstream debates tend to marginalize the local agency of host countries, and their developmental needs'. In fact, research has shown that China adjusts its approach to different political systems. For instance, in democracies such as Kenya and Ghana, China has adapted to their competitive and democratic digital ecosystems. Conversely, in more authoritarian contexts like Ethiopia and Rwanda, China has responded to local demands for surveillance and censorship. Said otherwise, the mainstream debate on China's Digital Silk Road:

> is rather Eurocentric and the developmental needs of developing countries when it comes to breaching digital inequalities and catching up in terms of digital infrastructure are often obscured. So today, the dynamic intersection between China and technological upgrading remains far from clear and requires more investigation: do Chinese tech giants create new opportunities for technology transfer, learning, and innovation or do they conversely hinder the building of technological capabilities in host middle-income countries?

To address this question, El-Kadi focused her research on North Africa – a key region for digital cooperation – and more specifically on Algeria and Egypt.

The 13th Five Year Plan published by the Central Committee of the Communist Party of China (2016, p.71) highlights the intention to 'develop an online Silk Road with the Arab countries and others'. Connecting China to Pakistan and extending to Marseille in southern France through East and North Africa, the PEACE (Pakistan East Africa Cable Express) cable epitomizes this strategy and qualifies North Africa as a priority area for Chinese digital investments. Huawei and ZTE have gained significant markets in the region, building 4G/5G networks and data centres as well as providing AI and cloud computing services. Notably, Huawei established a factory in Algiers to produce smartphones, and numerous data centres are being constructed in Egypt and Morocco.

Following a standard development economic framework and drawing on the work of Albert Hirschman, El-Kadi identified and traced the two main channels of technology spillovers in the Algerian and Egyptian ICT sector. In short, vertical spillovers occur between digital multinationals (such as Huawei) and local subcontractors, suppliers, and telecom operators. Horizontal spillovers, on the other hand, mainly happen through labour mobility: for example, an ICT engineer working for Huawei might move to a local company, leading to knowledge spillovers, particularly in managerial and technical knowledge. 'My research', explains El-Kadi, 'aimed at assessing not only whether technology and knowledge transfer occurred, but also what type of technology and knowledge is transferred, and if this contributed to technological upgrading in Algeria and Egypt'.

Regarding horizontal spillovers, El-Kadi found that there is a high level of labour localization in North Africa, primarily due to growing labour costs in China, and similar findings have been reported by other scholars in other regions of Africa, Latin America, and Southeast Asia. 'Labour localization is a positive step towards knowledge transfer', says El-Kadi; 'however, fieldwork findings suggest the existence of a glass ceiling for local employees, with top managerial positions all filled with Chinese nationals'. Overall, evidence of horizontal spillover is limited because most Algerian and Egyptian employees of ICT multinationals move between different multinationals rather than to local firms: 'employees working for Huawei, for example, often transition to competitors like Nokia, Ericsson, or Cisco within the country, or they move abroad. This trend limits the potential for knowledge transfer to local firms'.

As for vertical spillovers, El-Kadi continues, 'interviewed suppliers and subcontractors indicated that Huawei and ZTE provided them with training, as is often the case in the high-tech sector'. Yet:

> there was limited technology transfer, even in activities expected to be spillover-intensive, such as manufacturing: interviews with employees at the Huawei Algiers factory revealed minimal local value addition in the production of cell phones in that most components, including low-tech items like phone boxes, were imported from China. And this, of course, limits technology transfer.

Likewise, the training provided to local firms does not seem to have conveyed new knowledge that could help local technological upgrading. Instead, training appears to act as a socio-technical mechanism supporting the consumption of Chinese technologies and creating ecosystems of identifiable local firms able to install, troubleshoot, and maintain ZTE and Huawei equipment. The situation in terms of linkages with local universities is similar:

> Huawei is more active than other firms in providing training to university students in Egypt and Algeria. Although many high-level partnerships were signed to offer student training, the content focused mainly on troubleshooting and maintaining Huawei technologies rather than imparting cutting-edge knowledge that could enable local technological upgrading.

In sum, what El-Kadi's research shows is that China's digital presence in North Africa is primarily driven by demand, but local agency matters in determining the spillovers from Chinese firms in host countries, in that the way China shapes digital ecosystems depends on local political, economic, and cultural preferences. At the same time, emerging linkages between Chinese firms and the Algerian and Egyptian economies are reconfiguring ecosystems around the use of Chinese technologies and standards. Thus, El-Kadi concludes, 'there is an urgent need for more proactive policies from host governments because otherwise the Digital Silk Road risks creating new technological dependencies, locking local ICT actors into activities and relationships captured and defined by Chinese digital giants'.

PAPER PRESENTATION

Sovereignty and the three digital ecologies in an age of geopolitics

The paper presented draws from a chapter of the forthcoming book *In Search of a Unicorn? The Misplaced Aspirations of Strategic Autonomy in EU International Relations*, co-authored by Richard Higgott and Simon Reich (2025).

Kickstarting the second day of the symposium, **Richard Higgott** reflects on the ways in which digitalization has changed what it means for a state to call itself sovereign. In fact, 'the very idea of sovereignty is a polite fiction in times of globalization and digitalization', argues Higgott. Today 'many states confuse sovereignty with resilience and their struggle for policy autonomy' and with '*geopolitics* becoming the ideational watch word of an increasingly bifurcated (not bipolar) world order, the myth of sovereignty has grown again'. The result, Higgott continues, is that the 'illusion of sovereignty remains a determining factor in the organization of social and political life for states both great and small' – and the current discourse on sovereignty reflects 'the aspiration of states to rein in and harness their tech sector'.

Classical assumptions about sovereignty are no longer plausible, if they ever were. Indeed, as Stephen Krasner argues, sovereignty was never unlimited, undivided, and unaccountable. 'Sovereignty is not absolute. It is fungible', adds Higgott:

> it is more a process of bargaining in an increasingly hybrid international, globally networked context of digitalization – and networks, unlike traditional institutional hierarchies, encourage self-organization. If used responsibly, an open and transparent internet could be a force for good. But we have seen in previous panels how the democratizing hopes of the early 'Digital Utopians' have been challenged by digital technologies becoming agents of intrusion, control, repression, and political authoritarianism.

Driven by the monetization of behavioural data, digital technology casts a shadow over what it means to be free and equal in an age when both private actors and states have greater instruments of control. Digitalization extends political reach across borders and policy domains, making such borders and domains pivotal in states' desire to enhance *national* sovereignty via technological autonomy as opposed to via greater interdependence.

As Higgott goes on to explain, the relationship between digitalization and sovereign states can be thought of as characterized by hierarchy and hybridity. Hierarchically, there are three groups: 1) digital 'superpowers' (i.e. the US and China), 2) the aspiring great powers, notably Europe and, to a lesser extent, Russia and India, and 3) those dependent states that might be called the 'technology takers'. As for hybridity, we see it in the growing influence of non-state actors – some of which exhibit state-like properties – that have driven digitalization, most notably 'tech titans' such as Google, Apple, Facebook, Amazon, and Microsoft in the USA and Tencent, Huawei, Baidu, Alibaba, and Weibo in China. Against this backdrop:

> the battle to secure ascendancy is no longer simply between sovereign states competing across a spectrum from diplomacy to war. Rather, the major states are now harnessing powerful, privately developed technological platforms to enhance the rhetoric and practice of nationalism in the battle to assert their sovereignty, domestic power, and foreign policy influence.

Digitalization is a global phenomenon, but it is not a uniform process. Rather, Higgott identifies three competing visions of digitalization, or three *digital ecologies*: the American, Chinese, and European ecologies. 'Current tensions over design, governance, and jurisdiction of these three digital ecologies reflect, and are reflective of, broader global fissures', Higgott points out: the USA and China are now creating two sharply defined technological and online systems. The American model is primarily driven by the private sector and relies heavily on private investments, while the Chinese model is state-driven and thus depends on public investments. Both ecologies envelop the development of AI, big data, 5G, and instruments of cyber warfare within the context of their race for technological and digital hegemony, which lies at the heart of the wider strategic competition between the two countries. China's ambition extends beyond its simple authoritarian desire for an independent digital regime inside its Great Firewall: 'supported by Russia and Iran, China is keen to rewrite the rules of internet governance. Beijing wants the net in the hands of governments without global oversight, and not a global regulatory oversight regime'. In contrast, and not surprisingly, the US ecology reflects a more laissez-faire approach in which the internet is informally owned and largely regulated by American companies. 'The problem', however, 'is that domestic political divisions in the US inhibit a coherent, bipartisan policy in the development of cooperative regulation of data markets and data protection'. Moreover, it seems that Washington lacks a coalition of rule-making allies that share its vision of the internet and so 'the early "digital utopians" idea that competition driven by corporate actors practising transparency assists an open, transparent, secure (and in theory democratic) global internet would be attractive to other states has proven wrong'. And this, Higgott adds, raises an important question: 'Is a liberal conception of the global internet a bridge too far in a context where a centrifugal trend towards fragmentation accelerates as data become increasingly central to economic and national security and as a source of geopolitical power?'

For its part:

> the EU is attempting to crossbreed a third digital ecology: partially market-driven, with state regulatory efforts to contain the power of corporate internet actors and prevent national fragmentation of decision-making among its member states. In many ways, the EU has a more complex and perhaps sophisticated view of the role of markets than either of the two digital 'superpowers': the EU does not want an internet and related instruments of social communication operating in the techno-libertarian style of the US or the tight authoritarianism of China.

Instead, what the EU wants, according to Higgott, is a 'regulatory model', which Higgott sees as a euphemism for the (ideational) power to influence the international digital environment to compensate for the EU's lack of market share. Thus, the question for Europe is this: 'to what extent do competing US (under-regulated) and Chinese (over-regulated) approaches offer the EU space for developing its influence and reducing its dependence?' In sum, the EU's regulatory and dirigiste approach, epitomized by the GDPR, reflects its aspiration for digital sovereignty to be an essential element of its strategic autonomy, as also underscored by the words of President Macron: 'the battle we're fighting is one of sovereignty … If we don't build our own champions in all areas – digital, artificial intelligence – our choices will be dictated by others.'

Ultimately, what distinguishes each of the three digital ecologies identified by Higgott is the role of sovereignty and the question of whose sovereignty is being threatened or enhanced:

> Is it traditional sovereignty – meaning the state's autonomous control – that is at stake? Is it the independence of the new private-sector digital giants that Zuckerberg has compared to states? Or is it the 'individual sovereignty' of an increasingly marginalized citizenry?

There are clearly tensions between the three digital ecologies, and particularly between those of the two digital superpowers and the EU. In its search for Macron's 'sovereign control' in the digital policy domain, the EU is operating with a degree of intellectual innovation ahead of the two major players. EU strategy and policies have not been without some success, but what is not known is the degree to which they will act to stem the fragmentation of the wider global digital ecology in the longer term. The US has shown some signs of wishing to meet the EU on some of its privacy and data governance legislation. 'But it is not clear that either the political will or ability to secure change is sufficient in Washington', Higgott comments, 'and if it does not happen under a Democratic administration, it certainly will not happen under a Republican one'. On the other hand, befitting an authoritarian state, China is showing no desire to implement privacy agreements and data protection legislation that would weaken state control over the digital domain. At the same time, it is quite clear that the Westphalian system no longer constitutes a liberal international order. As Higgott points out:

> the myth of resilience and universalism is no longer tenable. The idea of a US-led order acting as propagator of Western universalisms is now openly in tension with an order based on territorial state-led activities, which emphasize bilateral sovereignty, borders, and group identities instead of the multilateral institutional agendas of the last part of the 20th century.

PANEL 4

Emerging voices in the digital domain

Taking their lead from the range of topics discussed in the first three thematic panels, four early-career researchers discuss their ongoing research in the digital domain. The first speaker in this last panel is **Stella Blumfelde**, who shares some of the findings of her PhD research and offers novel insights on digital governance and cybersecurity. As she explains:

> the current framework for cybersecurity governance spans across different international regimes and involves various security mechanisms. Progress in establishing a sound international framework for governing cyber insecurities is hindered by inconsistent and at times conflicting positions and interests among states as well as between states and non-state actors, inhibiting effective cooperation.

Yet, Blumfelde points out, 'with the changing character of international threats, individual states can no longer provide adequate security on their own'. As a result, international organizations have emerged as prominent actors in maintaining peace and security: 'International organizations possess the economic and human resources as well as expertise and technical capabilities to influence the ways in which societies and states articulate and address shared concerns on global matters, such as cybersecurity'.

Beyond the field of cybersecurity, international security governance has historically developed into a set of mechanisms or 'tools', all embodied and institutionalized in international organizations such as the UN. Initially, these included periodic meetings to deter aggression, and preventive diplomacy to settle disputes peacefully, followed by the establishment of sanctions, collective security actions, peace operations, and disarmament efforts. Today, Blumfelde points out, 'instead of dealing with security issues once they manifest, approaches anchored on the concept of resilience focus on equipping countries with the skills and solutions needed to understand, cope with, and manage security threats'. The resilience framework, Blumfelde explains, has been applied to a broad range of issues, from conflict to poverty and environmental concerns. Nowadays it is increasingly applied also to cybersecurity.

Within this context, the UN has emphasized the importance of regional organizations in building up states' resilience to cybersecurity threats and strengthening their overall cybersecurity frameworks. The way in which they do so is the focus of Blumfelde's ongoing research:

> In order to assess the role of regional organizations as security providers in the field of cybersecurity, I have developed my analytical framework from the perception that they act as complementary actors to the UN in security governance. This in mind, in order to understand the actorness or complementarity of regional organizations, my aim is to compare how cybersecurity governance tools differ between the UN and regional organizations.

The UN has developed a wide variety of tools to address international conflicts. In the context of cybersecurity, the UN employs confidence-building mechanisms that include 'the identification of governmental or cybersecurity expert points of contact to facilitate exchange of information and best practices, among which is sharing national views on political, legislative, and normative measures to protect critical infrastructure'. While the UN's efforts on the matter have been limited, it does employ capacity-building mechanisms for its member states, and these are crucial in the field of cybersecurity. These measures include, for example, training relevant national agencies to address ICT security incidents as well as providing legal or diplomatic support to mitigate cybersecurity threats. Finally, the UN has traditionally served as a platform to encourage and facilitate multistakeholder cooperation, which, through such platforms as the UN Group of Governmental Experts (UN GGE) and the UN Open-Ended Working Group (OEWG), holds true also in its efforts in cybersecurity governance.

Drawing on these observations, Blumfelde has focused her empirical research on five regional organizations: the Organization of American States (OAS), the African Union (AU), the Organization for Security and Co-operation in Europe (OSCE), the Association of Southeast Asian Nations (ASEAN), and the Shanghai Cooperation Organisation (SCO). As shown in the table below, these organizations apply largely the same security mechanisms as the UN. However, they do so 'with some peculiarities', as Blumfelde emphasizes: 'highlighted in red [in ***Table 1***], are the measures I have identified as being the key focus of regional cybersecurity governance. Moreover, bearing in mind the AU having established the Convention on Cyber Security and Personal Data Protection, this underscores the fact that regional organizations are not only complementary to the UN efforts in cybersecurity governance, they are very active actors in assisting and developing a common understanding in the region on these issues'.

Table 1
Regional cybersecurity governance

ORGANIZATION GOVERNANCE TOOLS	OAS	AU	OSCE	ASEAN	SCO
Confidence building mechanisms	X	X	X	X	X
Capacity building mechanisms	X	X	X	X	X
Multistakeholder cooperation	X	X	X	X	X
Technical measures	X				
Legal measures		X			

According to Blumfelde, these differences can be explained by a number of factors as identified in existing scholarly work within International Relations, including technological gaps between and within regions as well as differences in cybersecurity capacities across legal, technical, organizational, developmental, and cooperative dimensions. Moreover, there are different perceptions of what a cybersecurity threat actually is – or is not – which closely relate to different 'security cultures' and varied national interests, with some countries prioritizing economic growth over strict data privacy regulations.

From this preliminary comparative analysis and a number of interviews with cybersecurity policymakers, it follows that 'international cybersecurity governance should focus less on the global level – as is happening now – and more on the role of regional organizations within these processes, due to their geographic, cultural, and historical proximity to specific regions'.

Another conclusion that Blumfelde draws from her empirical research is that 'regional organizations should commit to defining what cybersecurity is, because conceptual misalignments could be one of the reasons why regional governance mechanisms diverge'. Besides, Blumfelde notes, while existing cybersecurity measures are often labelled as '*strategic* mechanisms', 'they do not fully encompass the multifaceted nature of cybersecurity, which also has dimensions linked to international conflict, human rights, and development, etc.', and so they hardly live up to what a resilience framework would entail.

Looping back to the broader discussion on digital authoritarianism, **Lorraine Charbonnier** outlines the conceptual contours of her ongoing research project on 'digital authoritarian *practices*' and explores possible new pathways through which to interrogate the relationship between digital technologies and authoritarian resilience.

Concerns over the rise of digital authoritarianism are increasing. Yet the very concept of 'digital authoritarianism' has not been clearly defined. 'This is not surprising', Charbonnier says, 'as ongoing discussions on digital authoritarianism mirror some of the conceptual shortcomings in the literature on authoritarianism more broadly'. In fact, authoritarianism is typically discussed as the opposite of democracy or as a residual category of 'non-democracy', and, when it comes to discussing its digital counterpart, 'instead of focusing on the phenomenon in its own right, the tendency is to look at what authoritarian actors do, often framing the issue as a struggle between democracies and autocracies'. As a result, according to Charbonnier, most of the ongoing debates operate with a limited conceptualization of digital authoritarianism, which carries with it some of the blind spots for which the scholarship on authoritarianism has already been criticized and which appears particularly relevant once transposed into the digital realm. For one thing, it is widely acknowledged that while all authoritarian regimes are non-democratic, each may be so in its own way – that is, 'authoritarian regimes may be authoritarian for very different reasons and in very different contexts. And this is likely to apply also in the digital world'. Second, the idea that 'free and fair' elections represent the key threshold for defining authoritarianism – which is itself problematic – cannot be transposed to the digital world:

> not only there are no 'digital' elections, but if we tried to look at digital authoritarianism through the lens of elections we would risk imposing a state-centric view in an environment where states may or may not be the key players, as we saw in previous panels.

The tendency to personalize regimes is also problematic: 'we should reconsider our fascination with "strongmen" for if it already leads to rather reductive conclusions in the analogue world, the complexities of the digital world make a narrow focus on individuals largely untenable'. For example, the Snowden revelations indicated that the US National Security Agency was gathering a vast volume of data on non-US citizens worldwide and:

> while this does not make the US an authoritarian regime, surely it can be interpreted as an authoritarian behaviour and, more importantly for the point I am trying to make, it has very little to do with individuals: the surveillance started under the Bush administration and continued through Obama's without any explicit order to initiate it; even the Congress was largely unaware of what was going on, and other governments were involved, too. In fact, hundreds of people were involved. It was not the doing of specific individuals or even regimes, but rather of a (transnational) configuration of actors, and part of the process may well relate to the unspoken beliefs that Kaspersen identified as *doxa* in her keynote speech.

Taking these remarks into account, Charbonnier suggests 'shifting the analytical gaze, at least momentarily, from "who does what" to "what is being done" and eventually "by whom"'. Said otherwise, she proposes focusing on 'digital authoritarian *practices*', offering the following working definition: 'Patterns of actions, embedded in a socially organized context and reliant on digital technologies, that are enacted to sabotage accountability by disabling people's voice and people's access to information through surveillance, control, and co-optation/manipulation'.

'There are of course many tools and techniques that can make for digital authoritarian practices, many of which have already been discussed by previous speakers', comments Charbonnier while presenting a preliminary and non-exhaustive taxonomy (see ***Table 2***). 'What the different categories of practices have in common', she continues, 'is that they all represent "technologies of government" in the broadest, Foucauldian sense of the term: they intend to "conduct the conduct" of people and societies'.

Table 2
Digital authoritarian practices

SURVEILLANCE	CENSORSHIP + TARGETED PERSECUTION	SHUTDOWNS	SOCIAL MANIPULATION AND DISINFORMATION
Passive surveillance (e.g. mobile phone tapping) **Targeted surveillance** (e.g. spyware) **AI and big data surveillance** (e.g. facial recognition systems) --- ***Surveillance laws and regulations*** (e.g. on data disclosure, retention and localization)	**Fear-based censorship and 'reprisal for digital expression'** (e.g. threats and risks of legal charges, detention, violence) **Friction-based censorship** (e.g. content blocking and filtering) **Infrastructure restriction** (e.g. firewalls) --- ***Censorship laws and regulations*** (e.g. onfake news, lèse majesté, sedition, indecency)	**Total internet shutdown** (national, subnational) **Partial internet shutdowns** (e.g. restricted websites, blocked apps) **Bandwidth throttling** (i.e. slowing of internet traffic) --- ***Laws and regulations on shutdown***	**Propaganda** **Disinformation** **Hate speech** **Trolling and harassment** to provoke or disrupt conversations **Doxing** to intimidate **Flooding** to sew confusion and overwhelm legitimate information sources **Automated methods** (e.g. bots and algorithms that create spikes in engagement) **Vandalism or defacement** (i.e. unauthorized acts to modify or obscure websites or accounts)

Different practices serve different purposes, build on different logics, rely on different digital technologies, and follow different time frames: some techniques, such as internet shutdowns, have an immediate impact but the longer they last, the less effective they become. Other techniques, such as disinformation operations, require a longer time frame to achieve maximum effect. ‘Each set of actions comes with its own benefits and costs, which shape decisions about what combination of practices gets enacted by whom and when’, Charbonnier points out, adding that ‘not every actor can do everything: choices are shaped by capacity, including but not limited to digital capabilities’. For example, recent research has shown that practices of disinformation and social manipulation are less effective in regimes with low legitimacy – ‘which is an intriguing insight if we consider varying levels of legitimacy across the spectrum of regimes and in light of concerns about democratic backsliding’. Further considerations pertain to the so-called ‘dictator’s digital dilemma’, whereby authoritarian regimes need to find a balance between their grip on society and the economic and political costs of maintaining such control in an interconnected, digitalized world. Similarly, Charbonnier ponders, ‘regimes formally on the more democratic side of the spectrum may consider the societal control enabled by (more subtle) technologies appealing and thus may also strive to find their way through their own digital dilemmas’.

In fact, while recent studies have confirmed that authoritarian regimes are more likely to enact digital authoritarian practices because they face fewer political constraints, empirical observations offer a more nuanced picture. Surveillance, for instance, is most prevalent in wealthy closed authoritarian regimes. Yet:

> when it comes to AI and big data surveillance, democracies are also quite active: passive and targeted surveillance provide tangible benefits in terms of control, but democracies face significant political constraints on enacting such practices. Yet the availability of more subtle techniques may alter the dynamic.

Another important insight stemming from this body of scholarship is that many states, especially those on the authoritarian spectrum, engage in more digital authoritarian practices than their capacities would suggest. This often means that they rely on external support and providers, which ‘highlights once again the crucial role played by private companies, who could then be seen as being de facto part of configurations of authoritarian actors, whether or not companies claim to be involved in politics. Notably, many of these companies are headquartered in democracies’. Perhaps even more interestingly, amid ongoing discussions about whether digital technologies reinforce authoritarianism or substitute for traditional authoritarianism, ‘recent research seems to suggest that whereas digital technologies reinforce long-standing authoritarian practices in highly repressive, closed regimes, in hybrid regimes those technologies tend to be more beneficial as substitutes’. Many insights may follow from this empirical finding. For one:

> we may come to realize that digital authoritarian practices might paradoxically reduce the need for authoritarian actors to enact blunt practices such as rigging elections or engaging directly in violent repression, making the inherent violence of authoritarian regimes less visible in the non-digital world.

Thus, the key point, Charbonnier concludes:

> is that examining how and why different actors combine various digital authoritarian practices may shed light on what we so vaguely call 'digital authoritarianism' and this, in turn, may help us devise better strategies to prevent, mitigate, and counter harmful practices, irrespective of who and what regime enacts them.

Delving deeper into a specific type of digitally enabled practices, **Alessandra Russo** explores some of the implications of applying emerging disruptive technologies in war contexts, discussing how 'algorithmic warfare' could have detrimental effects on democracy. As Russo explains, the rationale for her ongoing research is that these technologies – and particularly AI – are gaining traction and are increasingly used by states to ensure control within their own borders as well as to wage war. 'AI stands out', Russo says, 'because it transcends conventional technological paradigms due to its wide array of military and non-military applications, making it a general-purpose technology similar to the steam engine and electricity'. Russo's research aims to explore the issues underlying the deployment of military AI by democratic states, seeking to unravel their implications and the relationship between democracy and the use of advanced technologies in conflicts.

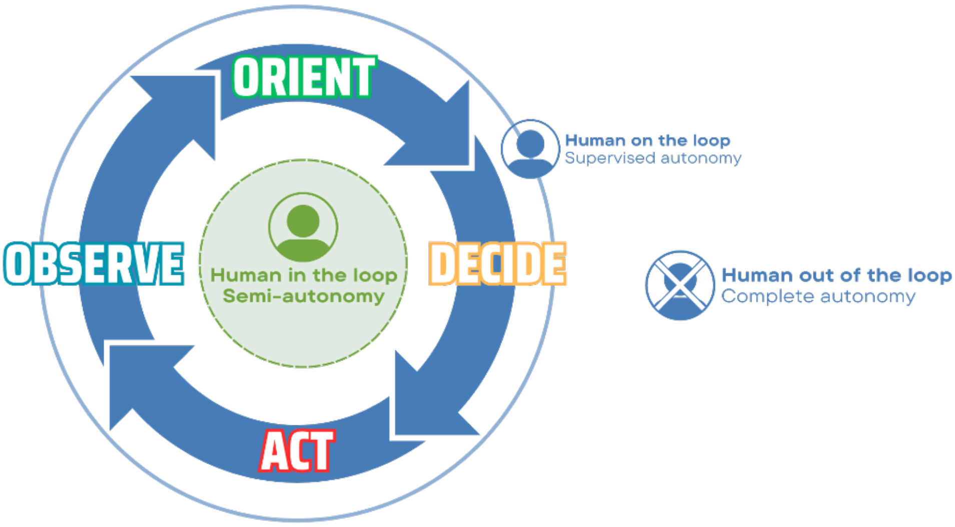
Indeed, as she argues, 'AI has the potential to enable more indiscriminate conduct of warfare, even by democratic countries'. This is so, Russo argues, because of a number of risk factors that are intrinsic to AI and its users. First and foremost are algorithmic biases stemming from flaws in underlying AI training data and in algorithm design, which can engender suboptimal or wrong outputs and, without proper scrutiny, can lead to major errors in decision-making and action. Second, and relatedly, are human biases, particularly the so-called 'automation bias': research in civil aviation has shown that in time-sensitive and cognitively challenging situations humans tend to over-rely on the output proposed by the AI systems without proper critical evaluation and scrutiny. Another risk factor stems from the fact that existing AI systems lack contextual understanding and are unable to engage in ethical considerations: an AI system might prioritize objectives such as minimizing casualties or achieving tactical goals without fully grasping the complexity of the situation and without considering the broader consequences of its actions. Lastly, the use of AI for sensitive tasks such as military targeting could reduce the direct involvement of human operators in decision-making processes, leading to reduced accountability and a detachment from the consequences of warfare, which in turn could potentially make indiscriminate actions easier to undertake or more likely to occur. As Russo explains:

> if we take these risk factors into account, the deployment of AI systems in warfare could enable three different phenomena: 1) lowered scrutiny over AI outputs, and 2) heightened decision speed (which is the main advantage AI offers), which together lead to 3) higher error and tolerance for collateral damage.

To demonstrate how this happens, Russo focuses her analysis on automatic target recognition (ATR) systems, pointing out that 'while mainstream narratives and public debates often fixate on lethal autonomous weapons systems, ATR is currently the AI application that is finding the broadest use in the military and that may have the most significant consequences'. Put simply, ATR refers to the use of computer processing to detect and identify targets automatically. These systems use data gathered from sensors – typically images – and data fusion to exploit geographical information, navigational data, geotags, internet-gathered information, suspected target locations, and target types. Through statistical analysis, ATR generates a list of targets – including people, buildings, and geographical areas – and prioritizes them by tactical or operational importance. Some of the most famous ATR systems are *Project Maven*, developed by the US, and the two Israeli software systems *Gospel* and *Lavender*, currently being used by the Israel Defense Forces (IDF) in the Gaza Strip. Each of these systems operates with a 'human in the loop' framework, meaning they are not used as completely autonomous systems (see ***Image 7***). However, there are significant differences in how this framework is implemented by the US and by Israel.

Image 7
'Human in the loop' framework

Source: Alessandra Russo



Established in 2017, *Project Maven* uses algorithms to identify personnel and equipment on the battlefield. The system can learn and autonomously refine its object recognition abilities through the analysis of training data and user feedback. Yet, 'as the Latin motto on its official badge conveys, there is no pretence for *Maven* to substitute humans in warfare: "*officium nostrum est adiuvare*" – "our job is to help"' (see ***Image 8***), Russo points out.

Image 8
Project Maven, official badge

Source: US DoD

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
officium nostrum est adiuvare
ALGORITHMIC WARFARE CROSS-FUNCTIONAL TEAM

So far, *Maven*'s deployment has been limited but it is expanding rapidly: trained and tested by data provided by drones and satellites gathered in counter-terrorism campaigns, *Maven* has been field-tested in the context of the Russo-Ukrainian war since 2022. In February 2024, the US used *Maven* in Iraq, Yemen, and Syria for retaliation strikes following an attack by Iranian-backed militants that killed three army reservists. Importantly:

> *Maven* is used for finding potential targets, not to verify them or deploy weapons against them – there is no automation in *Maven*'s functioning and every step the AI takes has a human checking in at the end. Instead, Israeli *Gospel* and *Lavender* operate quite differently.

Gospel and *Lavender* are two systems developed by the IDF for the identification of targets:

> These are not the first instances of AI being used by the IDF – for example, the '*Fire Factory*' has been in use since 2021 – but it is the first AI deployment in large-scale operations, namely the ongoing operations in the Gaza Strip.

The *Gospel* generates automatic recommendations for attacking private residences or buildings where suspected militants live or are believed to operate, whereas *Lavender* focuses on individuals (independent of location) to generate 'kill lists'. Both systems produce targets at a very fast pace with no significant or accurate scrutiny from human operators, who 'spend less than 30 seconds on any target before authorizing an attack, including the heavy shelling of private homes'. The IDF has been deploying its ATR systems with deliberate intent to exploit the speed of AI to the detriment of accuracy and scrutiny. Indeed, with *Gospel* and *Lavender*:

> there is no requirement to thoroughly check the output or the raw intelligence data – and this despite being aware that the system makes 'errors' in approximately 10% of cases, and that the system is known to mark as targets individuals who have only loose connections, or no connection at all, to militant groups – causing a high number of casualties.

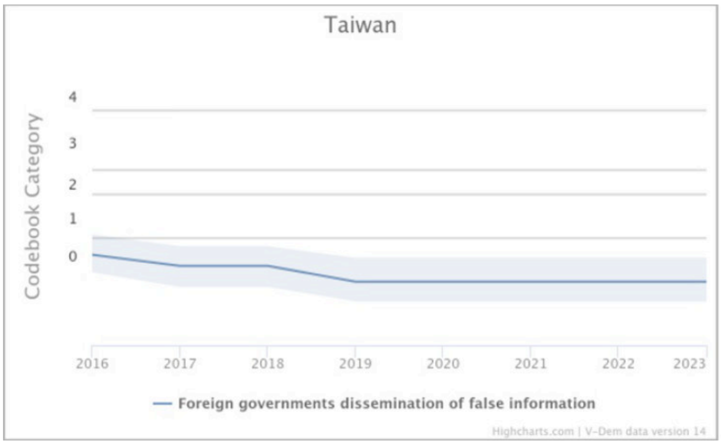
Hence, whereas the US has reportedly used *Maven* with meaningful human control, compliant with international humanitarian law (IHL), in the Gaza Strip we are witnessing 'a more dystopian use of these technologies whereby the choice to kill is de facto delegated to the machine and collateral damage is highly tolerated'.

In sum, the speed and operational advantage allowed by these technologies facilitate indiscriminate conduct in warfare, whether deliberate or not. Indeed, the intrinsic risks associated with AI make even unintentional indiscriminate use of offensive AI systems an issue to be reckoned with and addressed – especially as there is some indication that even the US intends to expand the autonomy of its algorithmic systems, including *Maven*, with the revision of Department of Defense (DoD) Directive 3000.09. What all this means is that even though democracies may formally uphold the protection of civilian lives and compliance with IHL and principles, the unchecked use of AI in conflict can de facto undermine the application of those very principles, highlighting the need to enhance accountability and transparency in 'algorithmic warfare'. This is all the more important and urgent, Russo argues, because:

> the urgency in conflicts or the fear of losing advantages to a competitor might push for a less careful or compliant AI deployment, and the misuse of AI might in turn lower the bar for other users' conduct and other states might exploit these precedents to deploy AI systems in noxious ways.

Graph 4
Foreign disinformation in Taiwan

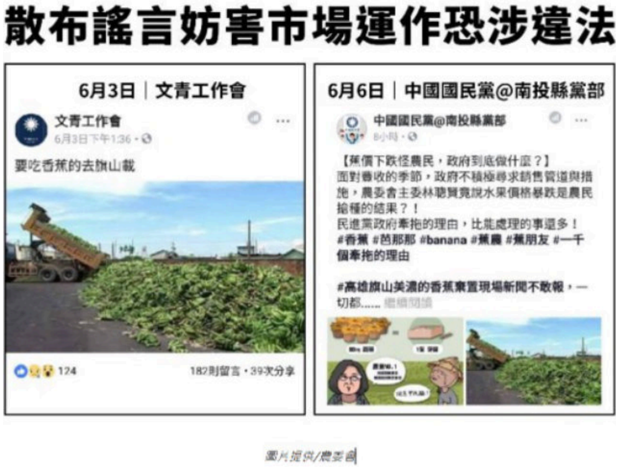
Source: The Digital Society Project/V-Dem



Closing the fourth panel, **Eton Lin** discusses the experience of Taiwan in devising ways to counter China's disinformation operations. Drawing on his own experience as a Taiwanese citizen, Lin recounts the differences between the two neighbours and the perceived threat posed by China to Taiwan: 'While there is no active conflict, information warfare occurs daily due to our shared language'. Indeed, a 2018 study by V-Dem (Varieties of Democracy) that uses a new set of indicators on social media and disinformation collected by the Digital Society Project demonstrates that foreign governments, especially China, disseminate false information on all major political issues in Taiwan. For example, China uses Taiwan's citizens and political parties to spread fake news ahead of elections, thereby interfering with the electoral process. According to the report, Taiwan has been seriously affected by foreign disinformation and it continues to be so to this day, ranking among the top countries facing such attacks from 2018 to 2023 (see ***Graph 4***).

During Taiwan's 2018 local elections, misinformation and disinformation were a severe issue. The Kuomintang (KMT), a political party also referred to as the Chinese Nationalist Party, used fake pictures showing farmers abandoning their produce, claiming that farmers could not sell it because of the Taiwanese government's poor performance (see ***Image 9***). 'During these elections', Lin says, 'Taiwanese citizens noticed a significant amount of fake news spreading on online platforms like Facebook, Instagram, Line, and WhatsApp, and demanded action from their government. The need for regulating online communication and countering disinformation became evident'.

Nevertheless, initially the government of Taiwan did nothing in response to China's disinformation attacks. According to Lin, the inaction can be attributed by the dilemmas emerging from the two main traditional approaches to countering disinformation: on the one hand, the 'US model' promotes a free internet, with governments relying on self-regulation by online platforms; on the other hand, the 'China model' advocates for each country's right to regulate its own cyberspace in light of what has been dubbed 'digital sovereignty'. As Lin explains,


散布謠言妨害市場運作恐涉違法

6月3日｜文青工作會

文青工作會
6月3日下午1:36・
要吃香蕉的去旗山載

124
182則留言・39次分享

6月6日｜中國國民黨@南投縣黨部

中國國民黨@南投縣黨部
8小時・

【蕉價下跌怪農民，政府到底做什麼？】
面對豐收的季節，政府不積極尋求銷售管道與措施，農委會主委林聰賢竟說水果價格暴跌是農民搶種的結果？！
民進黨政府牽拖的理由，比能處理的事還多！
#香蕉 #芭那那 #banana #蕉農 #蕉朋友 #一千個牽拖的理由

#高雄旗山美濃的香蕉棄置現場新聞不敢報，一切都…… 繼續閱讀

圖片提供/農委會

Image 9
Mis/disinformation during Taiwan's 2018 local elections
Source: Eton Lin

'while the first approach seems to be fundamentally flawed and ineffective as platforms often lack the incentive to regulate themselves, the second approach raises concerns about its authoritarian or anti-democratic underpinnings'. Therefore, Lin continues:

> the Taiwan government found itself faced by a dilemma: if it adopted the US model, the approach of self-regulation might not have been effective in protecting Taiwan from China's information warfare. But if it chose the China model, it risked aligning itself with China's cyber sovereignty theory, potentially endorsing authoritarianism as a means to counter authoritarianism.

The government of Taiwan found itself between a rock and a hard place, which explains the initial paralysis.

To address this dilemma, Taiwan had to move beyond traditional approaches to countering disinformation, adopting what Lin calls a 'civic-based approach' stemming from Taiwan's unique background. Since the late 1980s, Taiwan has become a more democratic and open society where non-governmental organizations (NGOs) and advocacy groups have flourished. Based on long-term observations of Taiwan's civil society post-democratization, renowned legal scholar Yeh Jiunn-rong coined the term 'civic constitutionalism' to describe the civic-centric, reform-minded movements driving constitutional change in Taiwan. Lin explains: 'Yeh Jiunn-rong emphasized that in considering constitutional issues, the role of citizens and civil society is crucial. Along the same lines, I argue that Taiwan's strategy against disinformation exemplifies civic constitutionalism'. Indeed, noticing the government's inaction against disinformation, Taiwanese civil society stood up: during the 2018 local elections, the Taiwan Media Watch Foundation and the Association for Quality Journalism established the Taiwan FactCheck Center to handle complaints about and investigate fake information. Shortly afterwards, other fact-checking services started to emerge (e.g. MyGoPen, Cofacts, Rumor & Truth, Auntie Meiyu, Doublethink Lab) and expose China's disinformation attacks.

Nevertheless, after the establishment of the FactCheck Center in July 2018, 'a battle over online disinformation regulation ensued between three key players: the government, civil society, and internet platforms', says Lin. On 10 October 2018, President Tsai Ing-wen emphasized in her National Day speech the importance of combating fake news. A few months later the Executive Yuan released a report on 'Preventing the Hazard of Fake News' that entailed four strategies: 1) enhancing citizens' media literacy and judgement, 2) creating mechanisms for clarification and third-party fact-checking, 3) collaborating with media platforms, and 4) holding individuals accountable for fake news through fair and independent judicial review. Internet platforms tried to resist, issuing an open letter through the Asia Internet Coalition arguing that the government's proposals would undermine freedom of speech. In response, the government urged platforms to take responsibility for self-governance, and indeed in June 2019 five platforms announced a Code of Practice for Self-Discipline for Preventing Misinformation. During this phase, civil society supported the government's decisions. Yet, when the government tried to tighten regulation on online communication and internet platforms, civil society pushed back. In June 2022, Taiwan's National Communications Commission (NCC) proposed a Digital Intermediary Services Act (DISA), inspired by the EU's Digital

Services Act, which would have empowered government agencies to apply to a court for ‘information restriction orders’ and ‘emergency information restriction orders’ to compel platforms to remove or restrict illegal content. Various NGOs strongly opposed the NCC’s proposed law, arguing that it excessively infringed on freedom of expression. The subsequent alignment between internet platforms and civil society led to the NCC withdrawing the DISA draft.

In sum, whereas the government at first hesitated to regulate online communication and counter disinformation, NGOs and citizens took the initiative, creating tools to identify false information and enhancing the general public’s media literacy. Through the two rounds of the ‘battle’ between key players, the efforts of civil society strengthened the government’s transparency, compelling it to provide more detailed and specific information about its policies. At the same time, civil society remained cautious of the government, and when it recognized the potential threat posed by the DISA to free speech, it took action to protect online autonomy. Drawing on Taiwan’s recent experience, Lin concludes, we may say that ‘civic constitutionalism represents a third approach to countering disinformation, showing that solutions transcend the binaries of “democracy vs authoritarianism” or “state vs market”’. Rather, effective solutions arise from the interactions among the state, market, and citizens: ‘instead of solely relying on or restricting private platforms, a good option to combat disinformation is to cooperate with empowered citizens, supporting and strengthening their initiatives instead of trying to replace them’.

Closing Remarks

Sharing his concluding thoughts, **Chris Alden** notes how the symposium has reinforced his belief that a multidisciplinary approach offers more insight than a narrow focus on disciplinary International Relations:

> By integrating various dimensions and perspectives, we have gained a more comprehensive understanding of the topic – an understanding which does not have to be always perfectly coherent. Engaging in discussions through multiple lenses and different disciplinary approaches was our initial intention, and the value of such an endeavour has been validated.

Indeed, **Stefano Ruzza** insists, echoing Alden's comment:

> over the last day and a half, we have covered a lot of ground. We have looked at our contemporary (digital) world from different viewpoints and at different levels of analysis. We have managed to fly high with concepts, get our hands dirty with practice and data, and sit with discomfort as we tackled uneasy dilemmas. And I think and I hope Christopher Coker would have been quite pleased with the outcome.

Day 1

Opening remarks

Stefano Ruzza

Associate Professor of Political Science and Peace and Conflict Studies, Università degli Studi di Torino; Head of Research, T.wai – Torino World Affairs Institute

Chris Alden

Director of LSE IDEAS; Professor of International Relations, London School of Economics and Political Science (LSE)

Nicolò Russo Perez

Head of International Relations, Fondazione Compagnia di San Paolo

Keynote speech

Anja Kaspersen

Senior Fellow, Carnegie Council for Ethics and International Affairs

PANEL 1 — Bad news: assessing and countering disinformation

CHAIR

Stefano Ruzza

Associate Professor of Political Science and Peace and Conflict Studies, Università degli Studi di Torino; Head of Research, T.wai – Torino World Affairs Institute

SPEAKERS

Michelagnelo Conoscenti

Professor of English Language and Linguistics, Università degli Studi di Torino

Massimiliano Fusari

Professor, H-FARM College; Visual Communication Strategist

Matthew Heneghan

PhD Candidate, University of Glasgow

PANEL 2 — Addressing Authoritarianism in Digital Governance

CHAIR

Chris Alden

Director of LSE IDEAS; Professor of International Relations, London School of Economics and Political Science (LSE)

SPEAKERS

Fang-Long Shih

Project Associate for the Digital IR in the Information Age project, LSE IDEAS

Antonella Seddone

Associate Professor of Political Science, Università degli Studi di Torino

Enea Fiore

PhD Candidate, Laval University and University of Geneva

Daniela Romée Piccio

Assistant Professor, Università degli Studi di Torino

PANEL 3 — Our Shared Digital Future: Recommendations for Public Private Cooperation

CHAIR **Vlad Zigarov**

Programme Manager for the IDEAS Europe Programme, LSE IDEAS

SPEAKERS **Kenddrick Chan**

Head of the Digital IR in the Information Age project, LSE IDEAS

Tin Hinane El-Kadi
PhD Candidate, London School of Economics and Political Science (LSE); Associate Fellow, Chatham House

Melanie Garson
Lead for Cyber Policy & Tech Geopolitics, Tony Blair Institute for Global Change; Associate Professor of International Conflict Resolution and International Security, University College London (UCL)

Day 2

PAPER PRES. — Sovereignty and the Three Digital Ecologies in an Age of Geopolitics

SPEAKER **Richard Higgott**

Distinguished Professor of Diplomacy, Brussels School of Governance; Visiting Fellow, Robert Schuman Institute at the European University Institute; Emeritus Professor of International Political Economy, University of Warwick

PANEL 4 — Emerging Voices in the Digital Domain

CHAIR **Davide Pellegrino**

Assistant Professor of Political Sociology, Università degli Studi di Torino

SPEAKERS **Stella Blumfelde**

PhD Candidate, Università degli Studi di Genova

Lorraine Charbonnier
PhD Candidate, King's College London; Research Fellow, T.wai – Torino World Affairs Institute

Alessandra Russo
PhD Candidate, Università Cattolica del Sacro Cuore

Yu-teng Lin
PhD Candidate, National Taiwan University

Closing remarks

Stefano Ruzza

LSE Ideas

twai
TORINO
WORLD
AFFAIRS
INSTITUTE

CPS
CULTURE
POLITICA
SOCIETÀ

UNIVERSITÀ
DI TORINO

With the support of

Fondazione
Compagnia
di San Paolo