Bus Inf Syst Eng 61(3):257–260 (2019)
https://doi.org/10.1007/s12599-019-00597-0

PROFILE

Interview with Erich Vad on "Political and Security Aspects of Digitization"

Stefan Pickl

Published online: 23 April 2019

Dr. Erich Vad
https://erichvad-consulting.de
https://de.wikipedia.org/wiki/Erich_Vad

Erich Vad was the Military Policy Adviser to the German Chancellor Angela Merkel and Secretary of the Federal Security Council in Berlin from 2005 to 2013. He lectured at the John Hopkins University and National Defense University in Washington, D.C. Erich Vad is the author of several monographs and numerous articles on contemporary strategy, security policy, management and leadership in national and international journals. Erich Vad lives with his family in Munich, works as a Business Consultant in Zurich and teaches at universities in Munich and Salzburg.

BISE: What changes does digitization bring about, in view of security, geopolitical, and strategic issues?

Vad: International power relations are rapidly diversifying; the global order is changing.

Prof. Dr. S. Pickl (✉)
Department of Computer Science, COMTESSA, Universität der Bundeswehr München, Munich, Germany
e-mail: stefan.pickl@unibw.de

The United States remains the world leader economically and militarily, as well as in scientific, technological, demographic, geographic and cultural issues. In addition to its leadership in outer space, the United States is also the leading power in digital and virtual space, with unrivaled international companies such as PayPal, Netflix, Amazon, Google, Microsoft, Apple, and Facebook. China is the only serious challenger to American leadership. Globally operating American corporations are unbeatable monopolies. They are expanding their activities to numerous other business fields such as autonomous vehicles, space travel, drones and artificial intelligence, without serious competition. "Winner takes all" is essentially the main business principle, and the hallmark of disruptive change in the age of digitization.

In the classical geopolitics of Halford Mackinder, Nicolas Spykman, Alfred Thayer Mahan, Zbigniew Brezinski and Henry Kissinger, the supremacy in Eurasia played a crucial role, i.e., dominance over opposite coasts in the Near and Middle East or control over maritime routes as well as the swift availability of a strong fleet. Unimpeded access to resources, which was, in the past, the hallmark of a world power, is still necessary, and must be supplemented by unhindered access to knowledge, data, and information. Ground-breaking digital technologies such as artificial intelligence and biotechnology have become strategic resources, and will continue that role in the future. Strategically important areas and regions were formerly conquered and occupied by sailors and soldiers, traveling merchants and missionaries; now and in the future, these are superseded by internet giants and their digital platforms.

Wealth and prosperity will increasingly be based on the strategic resources of knowledge, information, and communication.

It is no longer the dominance of territory by military bases and occupation forces that is the focus of geopolitics and strategy. Rather, it is about controlling and constantly influencing the unrestricted flow of knowledge, data and information.

The old, "analog" territorial principle in geopolitics will be replaced. Worldwide flows, such as the proliferation of information, energy, finance, trade, violence, weapons, and eventually people who voluntarily or involuntarily move around the world, change and complement classical geopolitical events. The ongoing digital transformation processes will fundamentally change international politics. In the US, as in China, a gigantic digital defense industry is being built. This consists mainly of critical digitized infrastructures such as secure energy and water supplies, government agencies and basically all sectors of industry.

In the digital domain, China denies unfettered access to its internet by American software companies and platforms through a "Great Firewall," as well as its own digital companies such as Huawei or Xiaomi. At its core, this strategy is about maintaining and defending political sovereignty. The strategy could also be an imperative for a digitally sovereign Europe. Looking at the possibilities and risks of digitization, one can say, (furthering Carl Schmitt's famous dictum) political sovereignty today is held by whoever dominates communication and the flow of digital information!

BISE: What do you see as the challenges of digitization with regard to political sovereignty and democracy?

Vad: The unobstructed availability of cyberspace and the integrity, authenticity, and confidentiality of the data it contains, have become existential issues and challenges of the 21st century. Without cyber-security and digital sovereignty, democracy, and the protection and security of a liberal political order, are ultimately not possible.

Political decision-making in a democratically organized society depends on security, confidentiality, and an open exchange of opinions. Cyber security and the preservation of digital sovereignty thus become central tasks and concerns for the state and its agencies. This also applies to international business enterprises, as well as to society, political decision-making, and democracy. Omnipresent digitization, immersion into completely different virtual realities, into very diverse digital information spaces, promotes the fragmentation of state and society.

The state runs the risk of being excluded as a sovereign actor from the sociopolitical decision-making process of the citizen. This applies worldwide to the majority of states, many of which are fragile domestically, and not a few of which have degenerated into veritable civil war, in which groups compete for control of the network. The unstoppable digitization of the world reinforces this mechanism.

The transparency in the network and the predictability of the behavior of citizens, by the use of "Operations Research", "Information Systems Engineering", "Big Data" and intelligent algorithms, increase the willingness of citizens to adapt. They want to avoid having a politically and socially undesirable profile on the internet and seek the desired, unimpeachable digital ideal. Especially in a digital democracy, the principle that the citizen may not be reduced to his digital personality profile must be maintained.

In the digital framework of free, open and democratic societies, one must always keep a *critical eye* on these potentially negative consequences and the social development potential that accompanies digitization.

An individual's personality must always be more than the sum of his network entries!

BISE: In your analysis of Federal security policy do you also consider the analysis of concrete data for political decision-making processes?

Vad: Data can be strategic. For a business, data loss can lead to loss of control over segments of the market, irreparable loss of reputation, and failure of the business. Political loss of control occurs when data security and protected communication no longer exist. Nonetheless, in the political arena, it is rather the evaluation of data that may be of interest to intelligence services.

WikiLeaks and the wiretapping of mobile phones, which I experienced as advisor to the Chancellor, show that there must be limits to the total digital transparency of our time. I also see a contradiction between the secretiveness of some software companies and the political postulates of some representatives of the digital avant-garde for transparency. Politics needs a certain amount of non-transparency, and needs some privacy to work out political positions and to prepare political decisions. Real-time data can impede sensible and balanced political discussion. We are confronted with conflicting narratives and world views in real time! The time pressure is enormous for political reaction to data and information, leading to a permanent race against the clock. Speed can lead to mistakes and rash political judgments. Government action often follows the digital "facts and figures," which often comes across as indecisiveness in the media.

Government action is not limited to responding to real-time data and information. After all, political action must be long-term and sustainable. It must not only "serve" the "loudest" who often live in very individual, digital bubbles, sometimes even in unrealistic surrogate realities. Government action is committed to the socio-political common good as a whole. The political *volonte generale* is more than the sum of fragmented, digital worlds of life and arbitrarily diverse political positions, which often have a high degree of willingness to change.

BISE: How do you rate the danger of "fake news" and the promised improvements that will be made available, for example, through "big data"?

Vad: Big Data aspires to be able to approximately predict human behavior. That's risky in politics. It overlooks possible daily moods and "good" opinions of the citizen. In the area of security policy, I would not rely solely on "big data." Who knows today what the security landscape of Europe and the world will look like at this time next year? Security policy and strategic action take place "in the dark of incalculability" – as Clausewitz once put it. You need more than only cognitive, rational intelligence. It also has a lot to do with empathy, emotionality and social intelligence, which largely elude measurability in the classical sense of Operational Analysis. In general, politics and political action can be very emotional and passionate and, as everybody knows, completely irrational, as statements and Twitter of some leaders show. However, "Big Data" can give early indications of changes in the international system, such as demographic changes or redistributions.

Turning off emotionality and intuition to obtain more security and political stability is also questionable. "Big Data" can certainly lead to new insights that will help us along the path of previously undiscovered correlations.

Certainly, they can refute or at least relativize some "fake news." But they can also lead to political behavioral adjustments and socially adapted or politically desired behavior. Exemplary here is the Chinese "citizen score," but also the increasing tendency in the digital age for "political correctness" in Western societies. While Karl Marx could still say that being determines consciousness, today it is close to saying that the digital image determines individual consciousness.

Digitization increases willingness to adapt to politically and socially desired, digital role models. Comprehensive, digital access to knowledge and information can hinder clear political positioning and promote political hedging. The state has lost its former mastery. That does not make government action easy in the age of digitization. Political sovereignty is also challenged given the monopoly position of international software companies and platforms. Ultimately, democracy and democratic will formation will only work if cyber security is guaranteed.

BISE: The current special issue of this journal is titled "Optimization and Data Analytics". Where do you see the greatest potential for optimization or in which area would you most like to see optimization?

Vad: Germany could use a great deal of optimization of its digital infrastructure and in the field of the Management and Use of Information and Knowledge. Despite being the leading economy of Europe, Germany has fallen desperately behind in terms of digital connectivity.

One can readily observe crossing the German border, not because of the border sign but because the wifi stops working.

Germany and Europe have slept through the digital revolution. In comparison to the United States and China, which possess nearly every tech giant, Europe threatens to become a mere appendage of either of these two great digital powers.

But it's not just a matter of upgrading Germany's wifi networks, the entire country needs to experience the full brunt of a digital revolution in the way Germany perceives information and uses analytics. Particularly, the government and state agencies are affected. Information sharing between state agencies at the state and federal level needs to increase. At the moment, it is practically non-existent. This is needed to ensure a secure documentation and integration of migrants, many of whom slip through the large gaps in Germany's current information system. Digital technologies are also necessary in German industry, where we face labor shortages due to demographic change. Additive manufacturing and digitalization of work processes, going so far as "dark factories" can help improve our quantitative and qualitative output while keeping our prices competitive on the global market. But the area of most urgent digital need is the military. The lack of reliable communication between the army, airforce and navy, as well as occasionally at the tactical level means a permanent tactical disadvantage and an inability to provide security for our allies and borders. To change all of this, Germany will have to change the way it views information. Legal barriers to the sharing of information will have to be swept aside to ensure the legal framework for digitalization to occur. A massive wave of investment in digital technology across all sector will have to take place. This will require both public and private investment.

It will most definitely force the government to abandon its "black zero" spending policy.

In the best case, the government makes this official policy with incentives for private stakeholders to participate. It will require the entire country to work together to make up for the ground we lost over the recent years.

BISE: There has been quite some hype about Artificial Intelligence. It has promised a lot. In your seminar on security policy, together with Prof. Pickl, you discuss the importance and relevance of AI with the students. How does the political science student handle it? Do you see this development as a "hype" or as a "new age"?

Vad: AI has had a big impact on politics in general and on security policy and strategy in particular. The US and China are the leading powers in AI, but many other countries, Russia and India, Singapore or Israel are investing heavily in AI, algorithm-based systems and robotics for both military and economic purposes.

Security policy makers can use AI to minimize misperceptions of a situation and its further development. Forecasting in the arena of security policy remains difficult, especially when thinking the global economy, the international system and its strategic impacts. National power derives in many ways from the intersection of economic power and military power. A strong economic base is necessary to sustain military and strategic advantages. AI can be used as a strategic decision-making aid as well as for controlling modern, autonomous security systems. Especially in this area, AI will revolutionize autonomy and robotics and replace earlier human decision-making bodies. The development of hypersonic systems, rockets and deep-penetration cruise missiles, currently being undertaken by the nuclear powers, will make AI-based battle management inevitable. There are virtually no more politically usable forewarning and reaction times and very limited, if any, defenses against these weapons. The role of decision support management and analysis, and the relationship between safety and security will change dramatically.

The use of AI can change international and strategic power relationships. Deterrence becomes more complex. This technological development is one of the reasons why international agreements such as the 1988 INF Treaty no longer have any relevance to our safety and that we need to think about new strategies. It will be a great challenge to ensure the political primacy of Clausewitz and to always bind the operational (OR-based) use of AI to the political and strategic level and thus to keep it politically controllable. Our well-known, conventional ways of political decision-making will change as a result. In any case, security policy and formulation of AI strategies are becoming increasingly diagnostic and will be constitutional part of a new field of Information Systems Design and Engineering.

AI supports strategic decision-making and helps to assess security policy and strategic changes. Especially in view of the disruptive, technological change potential due to AI, we need flexible, adaptable strategies, and a willingness to change those strategies as needed. Countries with leading companies in the arena of AI will have significant economic and strategic advantages.

In conclusion: AI will have a deep impact on economy as well as on defense, intelligence, social stability and the overall information environment. Countries that fail in this arena will inevitably lose their political, military and economic leadership.