KAS DISCUSSION PAPER

by **Benjamin Fricke**
Team Foreign, Security and European Affairs

GERMANY-ISRAEL STRATEGIC FORUM, DECEMBER 10-11, 2019, BERLIN
Session 3: THREATS IN THE CYBER SPACE

Cyber and the Future Balance of Power

Germany and Israel have long established deep economic and defence ties. A logical continuation of these would be a stronger cooperation between these two countries in the fields of cyber, Artificial Intelligence (AI) and computing advancements. While Germany continues its restrained foreign policy with its trade and business approach, Israel is also investing heavily in military AI, such as its combat vehicles and high-tech helmet displays. However, as civil and military uses are often based on the same research, many areas of cooperation can be found. Lastly, Israel and Germany will have no gains in a "balkanised" internet splintered between many different regions. Therefore, Germany and Israel should be in the driver's seat to propose a new digital framework for cyber security, such as a Schengen Agreeement for the internet.

German Interests

While the three global cyber and AI players, the United States, China and Russia are actively using big data for social and military advantages, Germany's cyber and AI strategy is more economic and trade based. For the country's current economic and political structure, this approach is the path of least resistance in terms of how to interact with the other (aforementioned) big players. However, such an approach also ensures that Germany will once again face familiar geopolitical problems, as it did in the pre-AI world. Who will guarantee the liberal world order and maintain the freedom of the seas to enable Germany's well-functioning AI-based economy to continue to export? The question of resiliency and self-defence will remain tied to the current query regarding Germany's NATO defence spending, which is supposed to be at two percent of Germany's GDP per year, yet does not reach this threshold. Will Germany also fall short in an AI world in terms of carrying its fair share for the future of democracy? And does the nature of AI, where security and economy are even more intimately related than before, permit tsuch a lapse? Is Germany prepared for this new type of warfare?

A small taste of this new warfare is the well-known case of Stuxnet, which is an example of the first cyber weapon being used. Purportedly developed by the US and Israel, it is believed to have done severe, albeit temporary damage to parts of the Iranian nuclear power programme. Iran, however, also has significant offensive cyber capabilities. For instance, Iran was able to penetrate the US Navy's unclassified computer network in 2013, remaining there for years even after its presence was discovered. Iran has also used wiper hacks, including an attack against the world's largest oil company, Saudi Aramco. When Chancellor Angela Merkel declared Israel's security as part of

Germany's *raison d' état,* she was probably not thinking of a cyber war at that point. However, this issue will become an integral part of that promise.

It is becoming an essential German interest to build up cyber, 5G and AI capable companies, and to ensure the country has trusted technology suppliers and reliable skills. Dependence on one single supplier is not a feasible situation for a high-tech economy such as Germany's, and would make it vulnerable to attack from all sides. National security interests aside, it is also a question of economic security to have an open component network, in which individual devices can easily be replaced with other company's products. Such products must, however, be trusted. All in all, Germany and Europe are in a fairly good position when it comes to high level AI research. However, the application of AI is often hampered by very restrictive privacy laws, i.e. big data is hard to access, and by a restrained foreign policy approach.

In conclusion, Germany's current interests can be summarised in four points:

1. **Industry 4.0:** The German economy depends on exports of high technology goods. Production processes must be as efficient as possible in order to maintain the competitiveness of German industry. This involves using innovative IT systems which enable entirely new production methods.

2. **Privacy:** One of the key challenges facing IT security is to develop processes and tools which enable members of the public to enforce their right to informational self-determination.

3. **Critical Infrastructures:** Many areas of social and economic life depend on efficient and reliable Information and Communications Technology (ICT) systems, and people's trust in their security. Deutsche Telekom reports around 45,000 attacks per day – and this number is increasing constantly. High priority must therefore be given to R&D projects into new solutions for IT security at critical infrastructures.

4. **Cloud Computing:** Cloud-based infrastructures that are distributed throughout the world offer attractive targets. New verifiable security concepts must therefore be developed and implemented in order to make full use of the potential of cloud computing.

Potential for Cooperation with Israel

German-Israeli cyber cooperation has already been in place for a few years, in various formats, such as the Hessian-Israeli Partnership Accelerator (HIPA) which focusses on developing solutions for securing 5G networks, preventing fraudulent e-mails and protecting internet infrastructures. Cyber-attacks are a daily reality affecting companies, public institutions, and private individuals. Ninety six per cent of all German small and medium-sized enterprises (SMEs) have already had

unpleasant experiences involving IT security incidents. Therefore, deeper and better funded research and development of cyber infrastructure, resilience and AI, as well as secure cloud storage are key issues of common interest to both countries.

Cooperation in the field of quantum computing is also important since this technology will affect AI and its applications. Quantum computing enable faster and more robust AI due to its massive computing power. The usage of quantum physics holds unprecedented potential for a global quantum computing network and the flow of data. From better message encryption to the design and analysis of molecules and teleportation of information, all these areas are crucial domains of cooperation.

For both Israel and Germany, cooperation in these fields can lead to economic and defence gains, technological advancement and the creation of a cyber-technology shield of deterrence.

Foreign Policy Options

National and regional players, such as the EU, Germany and Israel could start forming a more independent industry, and building up cyber and AI capabilities at home. Alternative markets should also be tapped into, such as South East Asia, Africa or South America. Nonetheless, it remains in the national interest – from a free market and defence point of view – to support competition in this field and to establish regulations, such as anti-trust laws regarding 5G technologies, and standards for AI as well as for cyber at large.

For Germany as well as Israel it should also be a foreign policy focus to maintain a single global internet and to prevent the "balkanisation" of cyber space into particular interests. The aim should be to preserve the vision of what the Obama administration described as an "open, interoperable, secure, and reliable internet."

Furthermore, Germany and Israel could be the driving nations behind a working replacement for the Budapest Convention; a form of Schengen Agreement for the internet. The member countries of such an agreement would work towards harmonising not only laws that deal with cybercrime, but also laws that define legal activity on the internet and promote digital trade. Such an agreement could, moreover, provide common rules for how data is stored and how it can be accessed by law enforcement agencies in the country where it is stored, the country where it is owned and by third-party countries. Such a multilateral agreement could provide far stronger and better mechanisms to deal with the downsides of open border cyberspace. Finally, real consequences and enforcement mechanisms for non-compliance ought to be applied, such as market access denial or black-listing of companies.