KAS DISCUSSION PAPER

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

KONRAD ADENAUER STIFTUNG

GERMANY-ISRAEL STRATEGIC FORUM, DECEMBER 10-11, 2019, BERLIN
Session 2: THREATS IN THE CYBER SPACE

Cyber and the Future Balance of Power

Germany and Israel have already established deep economic and defense ties for many years. A logical continuation 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 "balkanized" 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 Accord 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, yet it also ensures 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-defense will remain tied to the current one over Germany's NATO defense spending, which is supposed to be, but is not, at two percent of Germany's GDP per year. 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 that? Is Germany prepared for this new type of warfare?

A small taste of how this warfare may look like is the well-known case of Stuxnet which is an example of the first cyber weapon being used and is believed to have done severe, but only temporary damage to parts of the Iranian nuclear power program. Iran has significant offensive cyber capabilities. When Chancellor Angela Merkel declared Israel's security as Germany's *raison d' état,* she was probably not thinking of a cyber war at that point. However, this issue will become integral part of that promise. For example, Iran did penetrate the U.S. Navy's unclassified computer network in 2013 and was able to remain 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.

It is becoming an essential German interest to build up cyber, 5G and AI capable companies, and that it has trusted technology suppliers and reliable skills. A dependence on one single supplier is not a feasible solution for a high-tech economy such as Germany's and would make it vulnerable to attacks from all sides. Besides national security interest, 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. Those products must however be trusted. All in all, Germany and Europe at large are in a fairly good position when it comes to high level AI research, but research and application of AI is often hampered by very restricted 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 summarized 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 projects to research and develop 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 now in various formats, such as the Hessian-Israeli Partnership Accelerator (HIPA) which focuses 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 as well as private individuals. 96 percent 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 artificial intelligence as well as secure cloud storage are key issues of common interests.

Moreover, cooperation in the field of quantum computing is another important aspect, to advance in regard to AI and its applications. Quantum computing will change AI by giving massive computing power to enable faster and more robust AI. 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 aspects of cooperation.

For both, Israel and Germany, cooperation in these fields can lead to economic and defense technological advancement and create 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 build up cyber and AI capabilities at home. But also, alternative markets should be tapped into, such as south East Asia, Africa or South American. Nonetheless, it remains in the national interest from a free market and defense point of view to support competition in this field and establish a regulation of anti-trust laws regarding 5G technologies and Artificial Intelligence as well as cyber at large.

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

Furthermore, Germany and Israel could be driving nations behind a working replacement for the Budapest Convention, such as a Schengen Accord for the internet. The member countries of such an accord would work towards harmonizing not only laws that deal with cybercrime, but also laws that define legal activity on the internet and promote digital trade. A hypothetical accord should provide common rules for how data is stored and how it can be accesses by law enforcement 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 must be applied, such as market access denial or black-listing of companies.