Hybrid Warfare: Challenges for Intelligence Services

Dr. Peter Roell

April 2020

Summary

The author initially treated the present threat situation based on the various definitions of hybrid warfare, above all, how it is perceived by the US and the Peoples' Republic of China (PRC). Furthermore, he analyses various aspects of the problem such as China's espionage, Huawei and the challenges for intelligence services, hybrid warfare – terrorism – countermeasures, Germany's perception of the terrorism threat, Germany's counter measures, the role of the EU Intelligence Analysis Centre (INTCEN) in combating international terrorism, the importance of electronic warfare, some examples of electronic warfare in action, A2/AD technology and, finally, five recommendations.

ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

Definitions

I would like to introduce the present survey *Hybrid Warfare: Challenges for Intelligence Services* by way of two definitions.

Hybrid Warfare: There is no universally accepted definition of hybrid warfare. In his analysis *Conflict in the 21st Century: The Rise of Hybrid Wars,* Frank Hoffman, Research Fellow at the Center for Emerging Threats and Opportunities (CETO) points out that it is the simultaneous fusion of conventional and unconventional methods of conflict such as economic, military and informational instruments of influence.[1]

Wikipedia defines hybrid warfare as a "military strategy that employs political warfare and blends conventional warfare, irregular warfare and cyberwarfare with other methods of influence, such as fake news, diplomacy, and foreign electoral intervention. By combining kinetic operations with subversive efforts, the aggressor intends to avoid attribution or retribution. Hybrid warfare can be used to describe the flexible and complex dynamics of the battlespace requiring a highly adaptable and resilient response".[2]

I likewise find the definition "hybrid warfare" very useful to describe the combination of conventional, irregular and asymmetric means; such means include the persistent manipulation of political and ideological conflict, the combination of special operations and conventional military forces, intelligence agents, political provocateurs, media representatives, economic intimidation, cyber attacks, proxies and surrogates, paramilitaries, terrorists, and criminals elements.[3]

Intelligence agency: An intelligence agency is a government agency responsible for the collection, analysis, and exploitation of information that supports law enforcement, national security, military, and foreign policy objectives.[4]

Threat Perception

Intelligence services receive their intelligence requirements – whether in the political, economic, military technological or scientific spheres – from their respective governments. These, then, orient themselves at all times on the respective threat perception of states, whereby public information may also contribute to the situation report.

Over 1000 high-ranking international guests attended the Munich Security Conference from 16-18 February 2018. In an interview with Deutsche Welle radio, the conference's chairman, Ambassador (ret.) Wolfgang Ischinger, pointed out that the world was facing the most serious threat of military confrontation since the collapse of the Soviet Union in 1991.

---

[1] Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars", The Potomac Institute for Policy Studies, Arlington, Virginia, December 2007.
http://www.potomacinstitute.org/events/23-publications/reports/1267-conflict-in-the-21st-century-the-rise-of-hybrid-wars
[2] https://en.wikipedia.org/wiki/Hybrid_warfare
[3] Dr Peter Roell, "Migration – A New Form of Hybrid Warfare", ISPSW Strategy Series, Issue No. 422, May 2016.
http://www.css.ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/services/digital-library/publications/publication.html/e13bdd7d-8f57-4f79-9154-b2e489b9df68
Regarding Russia's hybrid warfare see: Markus Wehner, "Putins kalter Krieg – Wie Russland den Westen vor sich hertreibt", Droemer Knaur GmbH & Co. KG, München, 2018.
Boris Reitschuster, "Putins verdeckter Krieg – Wie Moskau den Westen destabilisiert", Econ Ullstein Buchverlag GmbH, Berlin, 2016.
[4] https://en.wikipedia.org/wiki/Intelligence_agency

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Among the several threats he cited as key dangers to global security were the risks of major conflicts in the Middle East, the nuclear standoff with North Korea and tensions between the West and Russia – in part, concerning the simmering conflict in eastern Ukraine. In another interview with a German journalist, he emphasized the deep mistrust between the military leaderships in Washington and in Moscow. The situation could hardly be worse.[5]

At an opening ceremony at the new Headquarters of Germany's Federal Intelligence Service (BND) in Berlin, on Friday, February 8, 2019, German Federal Chancellor Dr. Angela Merkel remarked that one of the key challenges for the BND was combatting hoax reports on the Internet. She pointed out that hoax information is used specifically as state propaganda. In her own words: "We must also learn how to approach and deal with fake news as part of hybrid warfare".

She also warned of cyber threats, that the protection of German IT infrastructures is consequently becoming increasingly important, and that many countries are particularly active in a war conducted via the worldwide network.[6]

The challenges faced by intelligence services have already become tangible from these findings.

But how do the United States of America and the Chinese leadership in Beijing see these threats? As the Chinese proverb says: There is no space for two tigers on the peak of a mountain.

So how did former United States Secretary of Defense, Jim Mattis, analyse the threat at that time? In January 2018 a close associate sent me a copy of the 2018 National Defense Strategy of the United States of America, which contained the following passage:

"We are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing, rules-based international order – creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.

China is a strategic competitor which uses predatory economics to intimidate its neighbours while at the same time militarizing parts of the South China Sea. Russia has violated the borders of nearby nations and pursues veto power over the economic, diplomatic, and security decisions of its neighbours. Meanwhile, North Korea's breaches of international law and reckless rhetoric continue despite United Nation's censure and sanctions. Iran continues to sow violence and remains the most significant challenge to Middle East stability. Despite the defeat of ISIS' physical caliphate, threats to stability remain as terrorist groups with long reach continue to murder the innocent and threaten peace more broadly."[7]

Ahead of the Trump-Kim Summit in Singapore on June 12, 2018, Washington repeatedly called for the complete, verifiable and irreversible denuclearization of the Korean Peninsula. In my opinion, however, Kim Jong-Un will never unilaterally abandon his nuclear weapons. His aim is a step by step approach to the lifting of sanctions and other economic benefits before decreasing North Korea's nuclear capabilities.

[5] https://www.dw.com/en/msc-chief-ischinger-warns-of-high-global-danger-of-war/a-42611829
[6] Frankfurter Allgemeine Zeitung, 9 February 2019.
[7] https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The second US-North Korea Summit between US President Donald Trump and North Korean ruler Kim Jong-un in Hanoi on February 27-28, 2019 failed for two fundamental reasons: Lack of diplomatic preparation at a working level, and failure by both sides to adhere to maximum demands.[8]

Looking at the outcome of the unexpected summit between President Donald Trump and North Korean leader Kim Jong-Un and the visit to the demilitarized zone (DMZ) on June 30, 2019, no real breakthrough was to be observed in the one-hour discussion in Freedom House. Their divergent definitions of denuclearisation remain unchanged.

The intelligence services in the USA will thus continue to optimize their intelligence activities in a difficult environment, and in cooperation with partner services. Germany's Federal Intelligence Service (BND) will also be able to improve its reconnaissance capabilities by procuring up to three spy satellites equipped with state-of-the-art technology. The goal of the Federal Government is to source its information efficiently and independently.[9]

References to hybrid warfare in the People's Republic of China can be found in the Annual Report to Congress *Military and Security Developments Involving the People's Republic of China 2019*, which states: "China's leaders employ tactics short of armed conflict to pursue China's strategic objectives through activities calculated to fall below the threshold of provoking armed conflict with the United States, its allies and partners, or others in the Indo-Pacific region. These tactics are particularly evident in China's pursuit of its territorial and maritime claims in the South China Sea as well as along its borders with India and Bhutan".[10]

Last year China also continued militarization in the South China Sea by placing anti-ship missiles and long-range surface-to-air missiles on outposts in the Spratly Islands, violating a 2015 pledge by Chinese President Xi Jinping that "China does not intend to pursue militarization".[11]

To analyse the Chinese perception, one must first see things from the perspective of the Chinese Politbureau. Like the Europeans, the Chinese have understood that there is obviously only one topic in Washington, in Congress, in the Pentagon, and in think tanks: China, China, China.

The *Global Times* has accurately described the quintessence of the dispute with the US, and what the Chinese leadership thinks:

"The recent row between the two major economies is not just about trade. In fact, all of the US requirements target issues beyond trade, which is actually meant to contain China's development in an all-round way. By curbing our development in the high-tech field, the US intends to manage China's future development in the way they design, thus posing serious challenges to us… More importantly, they don't want to see China develop high-tech industries, nor better their technology. That is to say, according to their design, changes must be made to the *Made in China 2025* initiative and to the reform of State-owned enterprises so as to contain China's

[8] Dr Peter Roell, "The Trump-Kim Summit in Hanoi: A Review", ISPSW Strategy Series, Issue No. 607, March 2019. http://www.css.ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/services/digital-library/publications/publication.html/8a52b32c-37fe-4e3e-8f26-775746c026ba
[9] https://www.zeit.de/2018/08/ueberwachung-bnd-satelliten/komplettansicht,
see also: https://www.zdf.de/nachrichten/heute/berichte-ueber-regierungsplaene-spionagesatelliten-fuer-den-bnd-100.html
[10] https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf
[11] Ibid.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

development."[12] And the *Global Times* claims that the PRC is ready to compromise on trade and other issues, but cannot give up the right to develop and relinquish their national sovereignty.

When acting Defense Secretary Patrick M. Shanahan declared before a House hearing in May 2019 that countering the threat posed by China is one of Pentagon's highest priorities, and identified Beijing's aggressive military build-up, systematic theft of technology, subversion of the rules-based international order and coercive global activities as key worries,[13] one may confidently assume that his statement contributed to the impression among experts of the Central Military Commission and the People's Liberation Army of being confirmed in their worst-case analysis.

Chinese President Xi Jinping had already raised the awareness of the military on January 4, 2019. In a key meeting of the Central Military Commission he ordered the PLA to intensify its training and preparation for war. The PLA must improve its joint operation capability, whereby new types of fighting forces should be the priority in the military's development, and more realistic training programmes must be introduced.[14]

Similarly, according to a statement of the U.S. State Department of July 8, 2019, that it has approved the possible sale to Taiwan of M1A2T Abrams tanks, Stinger missiles and related equipment at an estimated value of $2.2 billion, and thus that the present political tensions between Washington and Beijing is set to intensify.

On the same day, the Pentagon's Defense Security Cooperation Agency (DSCA) also notified US Congress of a possible arms sale to Taiwan, which could also include mounted machine guns, ammunition, Hercules armoured vehicles for recovering inoperative tanks, heavy equipment transporters and related support. It was also pointed out that this delivery of weapons would not alter the basic military balance in the region.[15]

I concur with this view, since the delivery of 108 M1A2T Abrams tanks as well as 250 Stinger missiles etc. would, indeed, not alter the basic military balance in the region, but would affect one of China's core interests. Washington will obviously continue to support Taiwan!

Hence, Chinese Foreign Ministry spokesperson Geng Shuang stated that the U.S. should immediately withdraw arms sales to and sever military ties with Taiwan so as to avoid further damage to bilateral relations and peace and stability across the Taiwan Strait.[16]

---

[12] Yossef Bodansky, "Rolling the Sleeves and Beating the Drums", Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), Issue no. 593, December 2018, p. 4.
https://www.ispsw.com/wp-content/uploads/2018/12/593_Bodansky.pdf
[13] Bill Gertz, "Shanahan outlines China threat", The Washington Times, 1 May 2019.
https://www.washingtontimes.com/news/2019/may/1/patrick-shanahan-outlines-china-threat/
[14] Yossef Bodadansky, "The Forthcoming Struggles and Wars According to Xi Jinping", Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), Issue no. 595, January 2019, p. 9.
https://www.ispsw.com/wp-content/uploads/2019/01/595_Bodansky.pdf
See also: Yossef Bodansky, "China-US: New Military Challenges in East Asia and Beyond", Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), Issue no. 603, February 2019.
https://www.ispsw.com/wp-content/uploads/2019/02/603_Bodansky.pdf
See also: "China Military Power – Modernizing a Force to Fight and Win", Defense Intelligence Agency 2019.
www.dia.mil/Military-Power-Publications
[15] Reuters World News, "U.S. State Department approves possible $2.5 billion arms sale to Taiwan", 8 July 2019.
https://www.reuters.com/article/us-usa-taiwan/u-s-state-department-approves-possible-2-2-billion-arms-sale-to-taiwan-idUSKCN1U32HT
[16] Kensaku Ihara and Tetsushi Takahashi, "China demands US scrap $2.2bn arms deal with Taiwan",
Nikkei Asian Review, 10 July 2019.
https://asia.nikkei.com/Politics/International-relations/China-demands-US-scrap-2.2bn-arms-deal-with-Taiwan

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Finally, some remarks regarding China's One Belt, One Road Initiative. EU officials are concerned that China is buying silence on Human rights and other issues that undermine the EU's ability to speak with one voice. Hungary, for example – where China is pledging to spend billions on a railway project – blocked the EU Statement on the South China Sea. Furthermore, EU officials are concerned that China will insist that countries receiving Chinese financial aid and assistance would be under obligation to accept Chinese standards and not EU standards which would, in turn, undermine European regulatory standards.[17]

China's Cyber Espionage

By way of introduction, I would like to point out that, naturally, other states likewise conduct espionage. Thus, for example, the US intelligence services are very active worldwide. My remarks deliberately focus on the Yellow Tiger, which spies on the White Tiger, as well as on the EU member states.

In December 2017, the German Federal Office for the Protection of the Constitution (BfV), Germany's Domestic Intelligence Service, issued a public warning that a Chinese intelligence service created thousands of fake profiles on the online platform Linkedin. Following a nine-month investigation, the BfV identified 10.000 German citizens who had been contacted by members of a Chinese intelligence service masquerading as employees of headhunting agencies, consulting firms, think-tanks or as scientists.

Recruitment targets were chiefly members of the German and European parliaments, but also senior diplomats, members of the armed forces, lobbyists, researchers in private or government think-tanks and political foundations. As former BfV President, Hans-Georg Maaßen, pointed out: "These individuals were all targeted as a broad attempt to infiltrate parliaments, ministries and administrations."

Many recruitment candidates were invited to all-expenses-paid conferences, or to fact-finding trips to this Asian country. The task of this intelligence service was to collect further information on their suitability for recruitment.

The press conference closed with the BfV urging European officials to refrain from posting private information on social media, since foreign intelligence operatives actively collected data on users' online and offline habits, gathering a range of information on the target person including hobbies and other interests etc.

It is quite plausible – given the importance attached to keeping face in Asia – that the government of the Chinese intelligence service dismissed the German allegations by claiming that the BfV's investigation was based on "complete hearsay" and was thus "groundless", before going on to urge German intelligence officials to "speak and act more responsibly".

Thanks to high-level government talks, a miracle occurred: recruitment activities were reduced dramatically.

According to BfV information, over 90% of the initial contacts failed in their desired objective; at over five percent, however, the number of continued first-contacts is thoroughly alarming. Even with a few successful operations in the targeted sectors, such as in politics and administration – but also in other affiliated fields, such

[17] Dr Peter Roell, "China's Interests and Challenges in the Mediterranean", paper presented at the workshop of the Konrad Adenauer Foundation *Security in the Eastern Mediterranean*, Athens, Greece, September 2018. https://www.ispsw.com/wp-content/uploads/2018/09/578_Roell.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

as in the economy, industry and the military – this could result in enormous damage to the Federal Republic of Germany.[18]

On 27 June 2019, the Federal Minister of the Interior, Horst Seehofer, and the President of the German Federal Office for the Protection of the Constitution (BfV), Thomas Haldenwang, presented to the public the 2018 Annual Report on the Protection of the Constitution – Facts and Trends.[19] I cite here the following passages from the above report:

"The focus of Chinese intelligence activities is shifting towards political espionage. Chinese intelligence services are now making great efforts to obtain information about supranational entities such as the EU and about international conferences, such as the G20 summit. Moreover, the country is very interested in policy positions on China, e.g. recognition as a market economy or territorial disputes in the South China Sea".

Intelligence targets continue to be business and industry, research, technology and the military. The same applies to the popular movements which the Chinese authorities call the "Five Poisons" – including the independence movement of the Uyghur and Tibetan ethnic minorities, the anti-regime Falun Gong movement, the democracy movement and proponents of sovereignty for the island of Taiwan – fearing that they threaten national unity and the Communist Party's monopoly on power.

In 2018, China continued to acquire medium-sized companies in the high-tech sector in order to close gaps in technology and carry out its ambitious high-tech programme "Made in China 2025", which is aimed at making China a global leader among industrialised nations. With this in mind, certain sectors and innovative technologies are targeted for support, including new energy sources and engines, medical technology, industrial robotics, information technologies and space and aviation technology.

The export of German high-tech could harm the German Economy in the long-run. Nor can it be ruled out that China, by acquiring security-relevant German Businesses, might obtain sensitive data and information which it could use to the detriment of German security interests.

Increasingly, the Chinese are attempting to exert political influence abroad. In late 2017, China's President Xi Jinping announced the start of a "new era" in which China would move closer to centre stage and become a global leader. He said the "China dream" would come true with the help of strategic master plans such as "Made in China 2025" and the "New Silk Road" project. The Chinese leadership has promoted the latter, also known as the Belt and Road Initiative (BRI), since autumn 2013. The project is intended to open land and sea routes connecting China, Africa and Europe, and was recently extended to include the Arctic and Latin America. It has also assumed a security policy.

The Chinese believe it necessary to ensure a favourable political environment for the project to succeed and are thus engaged in massive attempts to extend Beijing's global influence on politics, business, research and society. Governmental, semi-governmental and private Chinese actors use well-connected German decision-makers and multipliers to lobby on behalf of Chinese interests. Chinese investment in Germany also create economic dependencies which China can utilise as leverage to gain political concessions where necessary.

[18] Dr Roell, Peter, "The Importance of Electronic Warfare in a Disrupted World", Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), Issue No. 562, July 2018. https://www.ispsw.com/wp-content/uploads/2018/07/562_Roell.pdf
[19] Regarding the Chinese Intelligence activities see the *2018 Annual Report on the Protection of the Constitution*, Federal Ministry of the Interior, Building and Community, Berlin, June 2019, p. 296-302. www.verfassungsschutz.de; www.bmi.bund.de

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The increase in Chinese cyber attacks, as witnessed in 2017, continued into 2018. Meanwhile, attacks have become more difficult to detect. This development in the methods and techniques used by Chinese APT cyber attackers, in combination with a high level of resources, signifies a growing threat, which is also more difficult to identify.

The Chinese AP10 group is currently considered the most active group when measured by its visible activities and is currently focusing on targets in Japan and the USA, particularly in the telecom sector. The attacks are carried out in three stages: The initial attacks, which are difficult to detect, are followed by tactical reconnaissance on infected systems. The reloading of permanently usable harmful malware can then take place at any time, sometimes months after the initial infection. Methodology and software are individually adapted to the target spectrum or developed entirely from scratch.

Furthermore, as the BfV Annual Report 2018 indicates, so-called supply chain or managed service provider attacks are regarded as particularly effective and sophisticated. The aim is not to attack the target computer itself, which is usually well-secured, but to identify a detour via third parties installed in the target system and interfaces from service providers (e.g. for remote maintenance). Thus, by infecting presumably trustworthy programs and communication channels, malware can be smuggled through selected victim systems, whereby spyware can be reloaded at a later point in time.

Finally, the BfV states that the current world political situation and China's related political and economic ambitions lead one to expect a further intensification of espionage activities, as well as attempts to exert influence. Protecting German companies against cyber threats is the shared responsibility of government and industry. This is why the BfV continues to participate in the *Economic Security Initiative,* a forum for cooperation among security authorities and industry coordinated by the Federal Ministry of the Interior, Building and Community. This alliance is in an ongoing dialogue with those responsible for security in industrial associations and their member companies to prevent attacks against German industry".

The Federal Government has already provided the German intelligence and security services and other security agencies with personnel, material and financial resources, and will continue to do so to a considerable extent over the coming years. The challenge for the security services is to select qualified employees suited to such challenging tasks.

Huawei and the Challenges for Intelligence Services

On January 28, 2019 the US Justice Department announced criminal charges against Chinese telecommunications giant Huawei and its associates for nearly two dozen alleged crimes. The two indictments accuse Huawei of violating intellectual property law and lying about its compliance with US against Iran. Specifically, Huawei is charged with violating confidentiality agreements with T-Mobile by photographing, measuring, and stealing part of a T-Mobile-developed robot, as well as lying to banks about Huawei's ties with Iran affiliate Skycom so as to appear to comply with US sanctions. In addition, Huawei's CFO, Meng Wanzhou, was arrested on December 1, 2019 in Vancouver on charges of lying about violating US Sanctions against Iran, generating considerable backlash from Beijing.[20]

[20] European Values Think-Tank, "The US has charged Chinese telecom Huawei with violating intellectual property laws and lying about its compliance with Iran sanctions", Kremlin Watch Briefing, Prague, January 2019. kremlinwatch@evropskehodnoty.cz

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

In his speech at the Munich Security Conference (MSC) on February 16, 2019, U.S. Vice President Mike Pence urged allies to turn their backs on Huawei technologies, painting the Chinese telecommunications equipment supplier as a severe security threat. "Chinese law requires them to provide Beijing's vast security apparatus with access to any data that touches their networks or equipment. We must protect our critical telecom infrastructure, and the United States is calling on all our security partners to be vigilant and to reject any enterprise that would compromise the integrity of our communications technology or national security systems".[21]

Already on December 21, 2018, the Chinese Ministry of Foreign Affairs reacted with the following statement: "The Chinese government had never participated in or supported stealing of industrial secrets",[22] and urged Washington to withdraw its accusations.

The US is exerting strong, worldwide pressure on its allies and other states to prevent China from participating in the 5G project. The U.S. government, for example, is said to have threatened Germany with restrictions on the cooperation of the secret services in the event that the Chinese communications provider Huawei were to set up the new 5G data standard. In a letter to Federal Minister for Economic Affairs and Energy, Peter Altmaier, US Ambassador Grenell stressed that Huawei is obliged under Chinese law to serve Chinese security interests and that it will not be possible to minimise the risk of information being passed on to Chinese secret services through controls.

And indeed, Article 28 of the Chinese cyber security law states the following:

"Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with law".[23]

Undoubtedly, governments will task their intelligence officials to provide background information on the issue, so they can make political as well as economic decisions.

How does Jeremy Fleming, director of U.K. cybersecurity agency GCHQ, assess the threat situation?

In his address at the 35th IISS Fullerton Lecture in Singapore on February 26, 2019, he pointed out that security agencies must collaborate with governments so as to understand both the opportunities and threats presented by Chinese technologies, as well as the global nature of supply chains and service provision irrespective of the supplier's flag, and to obtain a clear view of the implications of China's technological acquisition strategy in the West. He added that GCHQ had been unambiguously clear with Huawei that it would be uncompromising on

See also: Department of Justice, Office of Public Affairs, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud", 28 January 2019.
https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial
See also: BBC News, "Huawei faces US charges: The short, medium and long story", 7 May 2019.
https://www.bbc.com/news/world-us-canada-47046264
[21] Ryo Nakamura, "Pence sharpens Huawei criticism in Munich security speech", Nikkei Asian Review, 17 February 2019.
https://asia.nikkei.com/Economy/Trade-war/Pence-sharpens-Huawei-criticism-in-Munich-security-speech
[22] Tsuyoshi Nagasawa and Oki Nagai, "China hits back at US allegations of mass cyberthefts", Nikkei Asian Review, 21 December 2018.
https://asia.nikkei.com/Politics/International-relations/China-hits-back-at-US-allegations-of-mass-cyberthefts
[23] Samuel Stolton, "Chinese cybersecurity law is a 'loaded weapon,' senior US officials say", 27 February 2019.
https://www.euractiv.com/section/cybersecurity/news/chinese-cybersecurity-law-is-a-loaded-weapon-senior-us-official-says/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

the security improvements it expected from the company.[24] He emphasised that the U.K. has yet to make a decision as to Huawei's inclusion in its domestic 5G network.

In speeches and other public appearances, the heads of MI6, GCHQ, and the National Cyber Security Centre have attempted to bring some clarity to the raging debate about Chinese technology. They all agree that there is a threat.[25]

On May 2, 2019 British Prime Minister Theresa May removed Gavin Williamson as defence secretary following leaked National Security Council discussions about allowing Huawei Technologies a role in building the country's 5G Network. The information, which was shared during an April 23 meeting of the National Security Council, concerned Huawei's possible involvement in developing the UK's 5G network. Shortly after the news broke, Williamson released a statement in which he "emphatically" denied any involvement in the break.[26]

Within the EU, however, there are also a number of critical voices regarding Huawei's equipment in new 5G projects. On 7 December, 2018, Andrus Ansip, Vice President of the European Commission and former EC Commissioner Digital Single Market stated that Europe should be worried about Huawei and other Chinese companies, given the mandatory cooperation they are obliged to maintain with Chinese intelligence services.[27]

And what of Germany's position? During his three-day visit to China in June 2019, Federal Minister for Economic Affairs and Energy Peter Altmaier also met Huawei's CEO Ren Zhengfei, in Shanghai. Almaier made it very clear that telecommunication security is top priority, and that all operators are to fulfil Germany's security requirements. It would be Huawei's duty to show that they are able to do so.[28] Already in March this year, speaking on a ZDF talk show he pointed out that Germany does not wish to ban Chinese telecoms equipment maker Huawei from building 5G networks.[29]

His statements comply fully with statements by German Chancellor Dr. Angela Merkel. "There are two things I do not believe. Firstly, to discuss these very sensitive security questions publicly, and secondly, to exclude a company simply because it is based in a certain country. The government has said our approach is not to simply exclude one company or one actor, but rather we have requirements of the competitors for this 5G technology".[30]

---

[24] Cloe Taylor, "China's role in 5G 'much bigger' than Huawei, British spy chief says", CNBC, 25 February 2019.
https://www.cnbc.com/2019/02/25/gchq-chief-addresses-risks-from-huawei-5g-and-chinese-technology.html
See also: Jeremy Fleming's Keynote Speech at the CYBERUK 2019, 24 April 2019.
https://www.gchq.gov.uk/speech/director-s-speech-at-cyberuk-2019
See also: Yossef Bodansky, "Huawei and the New Thirty Years War", ETH Zurich, December 2018.
https://css.ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/services/digital-library/publications/publication.html/65348b9a-cb49-4a00-a0a5-568196800208
[25] David Bond, "Huawei threat uncovers enemy within UK spy agencies", Financial Times, 1 March 2019.
https://www.ft.com/content/1e2089a0-3ab8-11e9-b72b-2c7f526ca5d0
[26] Deutsche Welle, "UK defense minister Gavin Williamson sacked over Huawei leak", 1 May 2019.
https://www.dw.com/en/uk-defense-minister-gavin-williamson-sacked-over-huawei-leak/a-48566923-0
[27] Jorge Valero, "Commission says Europe should be 'worried' about Huawei", EURACTIV, 7 December 2018
https://www.euractiv.com/section/eu-china/news/commission-says-europe-should-be-worried-about-huawei/
[28] Deutsche Welle, "Germany pressures Huawei to meet security requirements", 21 June 2019.
https://www.dw.com/en/germany-pressures-huawei-to-meet-security-requirements/a-49294841
[29] Deutsche Welle, "Germany won't ban Huawei from 5G auction", 8 March 2019.
https://www.dw.com/en/germany-wont-ban-huawei-from-5g-auction/a-47818771
[30] Laurens Cerulus, "Merkel pushes back on calls for Huawei ban in Germany", POLITICO, 19 March 2019.
https://www.politico.eu/article/merkel-pushes-back-on-calls-for-huawei-ban-in-germany/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Critical voices are also to be heard in the German media. Peter Limbourg, Director General Deutsche Welle, maintains that China does everything it can to block access to information, particularly from the foreign press. Consequently, permitting the Chinese firm to build Germany's 5G network is naïve, to say the least.[31]

Furthermore, the German magazine *Der Spiegel* points out in its article "Weniger verwundbar" ("*Less Vulnerable*") that in the German Christian Democratic Union (CDU) there is renewed opposition to the participation of the Chinese provider Huawei in the development of the mobile network 5G.[32]

I share the opinion of Prof. Dr. Patrick Sensburg MP, Member of the Parliamentary Control Committee (PKGr) "I do not trust the suppliers from China or the USA". One observes that the MP is well-acquainted with the subject of Intelligence!

In a *Der Spiegel* interview with Arne Schönbohm, President of the Federal Office for Information Security explains: "I think the risk is manageable. There are essentially two fears: first, espionage, such that data flows off unintentionally. We can counter this with improved encryption. Second, sabotage, such that networks are remotely manipulated or even turned off. We can also minimize this risk by not relying solely on one supplier in critical areas. With a possible market exclusion, we also increase the pressure on these providers".[33]

In January 2019, Polish authorities arrested Piotr Durbajlo and Weijing "Stanislav" Wang on charges of espionage on behalf of China. Wang, a Chinese national, was sales director at Huawei, while Durbajlo was a former member of the Polish domestic counterintelligence agency and former telecommunications advisor to Prime Minister Beata Szydlo. Durbajlo was well integrated into the senior level of the Polish government, and even designed the special smartphones.[34]

A Warsaw court agreed to prosecutors' requests to arrest the two men for three months. If found guilty of spying, they would face up to ten years in prison.[35] I have my doubts that this espionage case will have a deep impact on decision-makers in the European Union.

On 20 December, 2018, the U.S. indicted two Chinese nationals for carrying out cyber attacks and building "back doors" into telecommunications gear to steel military secrets. The department of Justice said the men stole intellectual property and confidential business information from more than 43 technology companies and government entities in the U.S., including the Navy and the NASA space agency; while on 21 December, 2018, China denied America allegations that Beijing has long-since been carrying out cyber attacks. Instead, Beijing accused Washington of espionage.[36]

Washington and Beijing will, naturally, not decelerate their intelligence activities, but rather increase them in the face of rising tensions.

Donald Trump's statement on the occasion of the G20 meeting (28-29 June, 2019) in Osaka is interesting.

---

[31] Peter Limbourg, "Opinion: Huawei's 5G plan for Germany is a bad deal", Deutsche Welle, 9 July 2019. https://www.dw.com/en/opinion-huaweis-5g-plan-for-germany-is-a-bad-deal/a-49528206
[32] Melanie Amann, Martin Knobbe, Marcel Rosenbach, Michael Sauga, Wolf Wiedemann-Schmidt, "Weniger verwundbar", Der Spiegel, No 30, 20 July 2019, p. 35-37.
[33] Ibid.
[34] Thomas Morley, "Huawei Espionage Arrests in Poland: A Wake-up call to Europe", the German Marshall Fund of the United States (GMF), 12 February 2019. http://www.gmfus.org/blog/2019/02/12/huawei-espionage-arrests-poland-wake-call-europe
[35] BBC News, "Poland spy arrest: Chinese telecom firm Huawei sacks employee", 12 January 2019. https://www.bbc.com/news/world-europe-46851777
[36] Tetsuro Kosaka, "China may be spying, but it learned from the best – the US", Nikkei Asian Review, 23 December 2018. https://asia.nikkei.com/Economy/Trade-war/China-may-be-spying-but-it-learned-from-the-best-the-US2

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

"US companies can sell their equipment to Huawei" – as long as the transactions do not present a "great national emergency problem."[37] It has yet to be seen whether the US Commerce Department would grant some temporary licences to US companies to resume business with Huawei. Within the European Union discussions are ongoing as to how to proceed with the Huawei project. Perhaps, at the end of this year we will obtain more detailed information.

The intelligence services of the European Union will continue seeking to obtain confidential information on the 5G topic. Even with secure information confirming that Chinese services are using Huawei to extract intelligence, policymakers must assess the extent to which it is advisable to block China, the strong economic partner, and shut out the billion-dollar business!

Hybrid Warfare – Terrorism – Countermeasures

In this section of my study I shall focus on Germany's terrorism threat perception and the role of the EU Intelligence Analysis Centre (INTCEN). Before continuing, I would first like to take a brief glance at Samir Abd Muhammad al-Khlifawi's master plan for the so-called Islamic State. Also known by his *nom de guerre*, Haji Bakr, he was the strategic head of the rebel group "Islamic State of Iraq and the Levant" (ISIL), and was former colonel in Saddam Hussein's Intelligence Services. He later joined the rebel group al-Qaida in Iraq and took part in the Iraqi insurgency.

In late 2012, he relocated to the small Syrian town of Tell Rifaat, north of Aleppo. From there he helped organize the capture of parts of Syria by the IS, which would, in turn, be used as a base for invading Iraq.

Under the guise of Islamic missionary centres, the IS opened bases and recruited informers by using hybrid warfare tactics. Khlifawi's plans aimed at gathering information on:

- the leading families and individuals in villages and towns;
- the source of the latter's income, weaknesses and secrets which would make them susceptible to blackmail;
- the rebel groups in villages or towns, their leaders and ideological orientation.

All such information was very helpful for expanding IS influence in Syria and Iraq. Haji Bakr was killed by rival rebels on January 6, 2014.[38]

Germany's Perception of the Terrorism Threat

In her speech, held at the 55th Munich Security Conference on February 16, 2019, Federal Chancellor Dr Angela Merkel pointed out that alongside strained relations with Russia, "the fight against terrorism is a major challenge for us". Consequently, Germany "will support the G-5 Sahel troops, which are striving to fight terrorism. We are engaged in Mali and are working to tackle terrorism there and are on the ground to train the armed forces".[39]

[37] Jackie Wattles, "Trump reversed course on Huawei. What happens now?", CNN Business, 30 June 2019. https://edition.cnn.com/2019/06/29/business/huawei-trump-us-goods/index.html
[38] See Haji Bakr, https://en.wikipedia.org/wiki/Haji_Bakr
[39] Speech by Federal Chancellor Dr. Angela Merkel on 16 February 2019 at the 55th Munich Security Conference. https://www.bundesregierung.de/breg-en/chancellor/speech-by-federal-chancellor-dr-angela-merkel-on-16-february-2019-at-the-55th-munich-security-conference-1582318

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Furthermore, at an opening ceremony at the new Headquarters of Germany's Federal Intelligence Service (BND) in Berlin, on Friday, February 8, 2019, the Chancellor emphasized that while IS has been pushed back, it has not disappeared, and has shifted its strategy to full asymmetric warfare. In view of the terrorist threat, collaboration with the US intelligence services is crucial.[40]

How does Thomas Haldenwang, President of the Federal Office for the Protection of the Constitution – Germany's Domestic Intelligence Service (BfV) – perceive the terrorist threat? In an interview with the German newspaper *Welt am Sonntag* on April 14, 2019, Haldenwang cautioned against underestimating the terror militia IS following its military defeat. One must at all times reckon with an attack in Germany. The headcount of potentially dangerous radical Islamists as classified by the BfV rose by 300 to 2240 in 2018, to which figure potential returnees must also be added. The IS persists, above all, in the form of a virtual cyber caliphate that incites attacks.

Maintaining an around-the-clock overview of all these people would be impossible, since as many as 40 civil servants are required per suspect. Attention is thus focused on those among them considered particularly dangerous.

The BfV is also concerned about the 300 children of German jihadists still living with their families in territories formerly held by IS terrorist militias in Syria or Iraq. At some point they will return to Germany after having experienced violence and been subject to indoctrination.

Attempted attacks in recent years indicate that adolescents could become assassins at an early age. For this reason, Haldenwang called for amendments to the law allowing for children to be monitored on a case-by-case basis.[41]

At this point I would like to present a few examples of terrorist attacks in Germany, but also against German citizens in other countries.

The most devastating terror attack in Germany took place on 19 December, 2016 when the terrorist, Anis Amri, hijacked a truck and murdered the driver before plunging the truck into the Christmas market at Breitscheidplatz in Berlin. Twelve people died, more than 60 were wounded, some of them seriously. The IS claimed responsibility for the attack. Four days later, Anis Amri was killed in a shootout with police near Milan, Italy.[42]

On 24 July, 2016, a twenty-seven- year-old Syrian Asylum seeker, Mohammad Daleel, detonated himself outside a wine bar in the German town of Ansbach. He had been refused entry to a music festival when failing to produce an entrance ticket. Fifteen people were injured in the blast, four seriously. Daleel was in contact with the IS and had been planning attacks before his backpack accidentally exploded.[43]

On 22 July 2016, eighteen-year-old Ali David Sonboly, of dual nationality (Iranian-German) carried out a shooting in the vicinity of the Olympia shopping centre in Munich. Ten people were killed, including the perpetrator, and 35 others injured. He was located by police approximately one kilometre from the shopping centre where he

[40] France 24, "Contradicting Trump, Merkel says Islamic State group 'far from defeated'", 8 February 2019. https://www.bundesregierung.de/breg-en/chancellor/speech-by-federal-chancellor-dr-angela-merkel-on-16-february-2019-at-the-55th-munich-security-conference-1582318
[41] Interview *Welt am Sonntag* with Thomas Haldenwang, 14 April 2019, p. 4.
[42] Wikipedia, "2016 Berlin truck attack". https://en.wikipedia.org/wiki/2016_Berlin_truck_attack
See also Marcel Fürstenau, "Berlin Terror Attack: Germany Grapples with Unanswered Questions Two Years on", Deutsche Welle, 19 December 2018. https://www.dw.com/en/berlin-terror-attack-germany-grapples-with-unanswered-questions-two-years-on/a-46802429
[43] Wikipedia, "2016 Ansbach bombing". https://en.wikipedia.org/wiki/2016_Ansbach_bombing

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

killed himself. Though not motivated by the IS, Sonboly had psychological problems, and admired people who committed amok-attacks.[44]

On 18 July, 2016, a seventeen-year-old refugee, Riaz Khan Ahmadzai, also known as Mohammad Riyad, severely injured four tourists from Hongkong with a knife and a hatchet on a regional train near Würzburg. A fifth person was injured outside the train once it had stopped and the attacker sought to flee the scene. He was later shot by a Special Forces Commando. The IS claimed responsibility for the attack.[45]

I would like, furthermore, to present two examples were German citizens were killed by terrorists in Turkey and France.

On 12th January 2016, the terrorist Nabil Fadli (28) walked up to a group visiting Sultanachmet Square in the historic centre of Istanbul and detonated himself, killing thirteen people including twelve Germans. Fadli entered Turkey from Syria on 5 January and was registered and fingerprinted as a refugee. At that time, his name had escaped security alerts. Fadli was a member of the IS.[46]

On the evening of 14 July, 2016, 85 people were killed and 308 injured when a cargo truck was deliberately driven into crowds celebrating Bastille Day on the Promenade des Anglais in Nice, France. The driver, Mohamed Lahouaiej-Bouhiel (31), was a Tunisian national resident in France. The terrorist was finally shot in the ensuing gun battle with police. The IS claimed responsibility for the attack.[47]

Germany's Counter Measures

That security agencies cannot prevent all terrorist attacks is a platitude. Here, I would like to mention three examples of the successful work of the security services.

Following an extensive nine-month investigation involving over 600 agents, a bomb plot by the Islamic Jihad Union (IJU) affiliated Sauerland terrorist cell was discovered; this was primarily thanks to the intercepted communications between the IJU members. Three men were arrested on 4 September 2007 while leaving a rented cottage in the Oberschledorn district of Medebach, Germany, where they had stored 700 kg of a hydrogen peroxide-based mixture and 26 military-grade detonators. They were attempting to build car bombs.

A supporter was later arrested in Turkey. All four had attended an IJU training camp in the border region between Afghanistan and Pakistan in 2006. They were planning terror attacks at Ramstein Airbase, Frankfurt Airport and other public locations.

Thanks to the intercepted communication by the NSA, and the sharing of their knowledge with Germany, this counter-terrorist operation proved very successful.[48]

The arrest of terrorist suspect and Syrian refugee Jaber al-Bakr on Monday, 10 October, 2016 by the Leipzig police, underlines the terrorist threat in Germany. Al Bakr planned to execute a terrorist attack at Tegel Airport

[44] Wikipedia, "2016 Munich shooting". https://en.wikipedia.org/wiki/2016_Munich_shooting
See also Janek Schmidt, Kate Connolly, Emma Graham-Harrison, "Munich shooting: killer was bullied teen loner obsessed with mass murder", The Guardian, 24 July 2016.
https://www.theguardian.com/world/2016/jul/23/munich-shooting-loner-facebook-ali-sonboly-bullied-killer
[45] Wikipedia, "Würzburg train attack". https://en.wikipedia.org/wiki/W%C3%BCrzburg_train_attack
[46] Wikipedia, "January 2016 Istanbul bombing", https://en.wikipedia.org/wiki/January_2016_Istanbul_bombing
[47] Wikipedia, "2016 Nice truck attack". https://en.wikipedia.org/wiki/2016_Nice_truck_attack
See also: BBC News, "Nice attack: What we know about the Bastille Day killings", 19 August 2016.
https://www.bbc.com/news/world-europe-36801671
[48] Wikipedia, "2007 bomb plot in Germany". https://en.wikipedia.org/wiki/2007_bomb_plot_in_Germany

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

in Berlin and had already organized all the necessary explosives. On Wednesday, 12 October, he committed suicide in his cell.[49]

On 7 June 2019, the trial of a Tunisian national and his German wife began in Dusseldorf. The couple, "Islamic State" followers, have been charged with preparing a terrorist attack with ricin, 6.000 times more lethal than cyanide. They aimed to "kill and wound the largest number of people".

The raid came after a tipoff from the US Central Intelligence Agency (CIA), whose monitors had noticed the large online purchase of 3.300 castor beans. A small amount of ricin in natural form is found in castor beans.[50]

Since 2016, German security authorities have prevented seven planned terror attacks in my country. In some cases, 200 security personnel have been involved, including interpreters of different dialects.

To combat international terrorism, the German Government set up the Joint Counter-terrorism Centre in 2004 in Berlin, a joint co-operation and communication platform used by 40 domestic security agencies. In daily briefings and various working groups, these groups assess the current situation trend and security-related incidents. The aim is to identify potential Islamist threats at an early stage and to take comprehensive action against concrete dangers.[51]

In April 2018 the Federal Minister of the Interior Horst Seehofer visited the Joint Counter-Terrorism Centre (GTAZ); in a press conference following the meeting he pointed out that the GTAZ performed excellently. He announced that the security authorities will receive more staff and resources, but also greater powers. For example, the BKA is to receive a new division devoted exclusively to counter terrorism.[52]

The Role of the EU Intelligence Analysis Centre (INTCEN) in Combatting International Terrorism

Intelligence analysis within the European Union is not a new phenomenon. In the Treaty of Amsterdam of 1997, one reads in paragraph 6.5 of the Declaration on the Establishment of a Policy Planning and Early Warning Unit, that member states and the Commission are to assist the policy planning process by providing relevant information, including confidential information, to the fullest extent possible.

When posted to the Permanent Representation of the Federal Republic of Germany to the EU in Brussels in 2001, I had the privilege of following developments in intelligence analysis within the EU.

In the wake of the terrorist attacks in New York and Washington of 11 September 2001, the then High Representative for Foreign Affairs and Security Policy, Xavier Solana, decided to use the existing Joint Situation Centre (SITCEN) to start producing intelligence based on classified information.

On Solana's request, in June 2004 the Council of the European Union agreed to establish a counter-terrorism cell within the SITCEN. This cell was tasked to produce counter-terrorist intelligence with the support of the member states.

[49] BBC News, "Syrian terror suspect Jaber al-Bakr found dead in cell in Germany", 12 October 2016. https://www.bbc.com/news/world-europe-37638631
[50] "Ricin attack plot trial starts for Tunisian-German couple", Deutsche Welle, 7 June 2019. https://www.dw.com/en/ricin-attack-plot-trial-starts-for-tunisian-german-couple/a-49097871-0
[51] Bundesamt für Verfassungsschutz, "Gemeinsames Terrorismusabwehrzentrum (GTAZ – Joint Counter-Terrorism Centre)". https://www.verfassungsschutz.de/en/fields-of-work/islamism-and-islamist-terrorism/gtaz-en
[52] Federal Ministry of the Interior, Building and Community, "Federal Minister Seehofer visits Joint Couter-Terrorism Centre", 12 April 2018. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2018/04/visit-gtaz.html

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

As of 2012, the EU INTCEN is composed of two divisions:

- The Analysis Division is responsible for providing strategic analyses based on input from the security intelligence services of the member states. It is composed of various sections that treat geographical and thematic topics.
- The General and External Relations Division deals with all legal and administrative questions, as well as open sources analyses. It is composed of three sections each of which deals with IT questions, internal and external communication, as well as open source analysis.

In December 2015, Federica Mogherini, High Representative for Foreign Affairs and Security Policy and Vice President of the European Commission, appointed Dr. Gerhard Conrad as the new Director of the EU Intelligence Analysis Centre (INTCEN) at the European External Action Service (EEAS).

The latter formerly held high-ranking posts in the German Foreign Intelligence Service (BND), speaks fluent Arabic and holds a doctorate in Islamic studies. He assumed his post in January 2016.

Among his chief tasks are the strengthening of cooperation between European Intelligence Services, and the provision of valuable strategic analyses to EU decision-makers, including topics in and around international terrorism.

What are the advantages of intelligence cooperation in the European Union?

Information provided by the foreign and domestic intelligence services of the EU member states to the INTCEN has the following merits:

- Intelligence information is garnered from different intelligence and security services, and the various expertise are pooled;
- the overall knowledge-base is consistently augmented;
- the perceived threat is uniformly monitored;
- the common analysis process is fostered, and joint political decisions are supported.

INTCEN maintains further ties with the European Union Satellite Centre (EUSC) in Torrejon, Spain, the European Police Office (EUROPOL) in The Hague, EUROJUST (likewise in The Hague), the EU Institute for Security Studies (EUISS) in Paris, and the European Union Agency for Network and Information Security (ENISA) in Heraklion, Crete, with its expertise in cyber security. Furthermore, INTCEN liaises with the foreign offices and the ministries of the interior of the EU member states and is able to draw on the expertise of the special representatives in the relevant regions.

More than 100 analysts, including cyber experts from the foreign and domestic intelligence services of the EU member states, are now operative within INTCEN.

The Importance of Electronic Warfare

Electronic Warfare (EW) involves the use of electromagnetic spectrum, or directed energy, so as to control the spectrum attack of an enemy or impede energy assaults via the spectrum. The purpose of electronic warfare is to deny the opponent the advantage of, and ensure friendly unimpeded access to, the EM spectrum. EW can be

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

applied from the air, sea, land and space by manned or unmanned systems, and can target humans, communications, radar, or other issues. Electronic warfare includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).[53]

According to NATO, the purpose of EW is to deny the opponent the advantage of and ensure friendly unimpeded access to the electromagnetic spectrum. EW can be applied from air, sea, land and space, and target communication and radar systems. It involves the use of the electromagnetic energy to provide improved understanding of the operational environment as well as to achieve specific effects on the modern battlefield.[54]

I would like to start by taking a brief look at the world military expenditure in 2018. According to the Stockholm International Peace Research Institute (SIPRI), it has increased to $ 1.8 trillion, and thus highlights the critical situation currently experienced in many regions of the world. US military spending grew – for the first time since 2010 – by 4.6 per cent, to reach $649 billion. The USA remained by far the largest military spender in the world.

China, the second largest spender in global comparison, increased its military spending by 5.0 per cent to $250 billion in 2018. India increased its military spending by 3.1 per cent to 66.5 billion. Pakistan's military spending grew by 11 per cent to reach $11.4 billion, while South Korea's spending rose to $43.1 billion, an increase of 5.1 percent. Major drivers for the continuing growth of military expenditure in the region are the rising tensions between the US and China, but also tensions between Asian countries.

Russia's military spending decreased by 3.5 per cent compared with 2017 and reached $61.4 billion in 2018, perhaps due to economic problems. In Central and East European Countries, a large increase could be observed. Military spending in Poland rose by 8.9 per cent in 2018 to 11.6 billion, while spending by Bulgaria, Latvia, Lithuania and Rumania ranged between 18 to 24 per cent. It is not surprising that military expenditure by the Ukraine was up by 21 percent to 4.8 billion owing to the tense relations with Russia. Total military spending by all 29 NATO members was $963 billion in 2018.

Six out of ten countries with the highest military burden in the world are in the Middle East: Saudi Arabia 8.8 percent of GDP, Oman 8.2 per cent, Kuwait 5.1 per cent, Lebanon 5.0 per cent, Jordan 4.7 per cent and Israel 4.3 per cent. Most striking is the high defence expenditure of Turkey with an increase by 24 per cent in 2018 to $19.0 billion.

In Africa military spending fell by 8.4 percent in 2018; in South America it rose by 3.1 percent, mainly due to the increase in Brazilian spending (5.1 per cent).[55]

In this environment, it is interesting to note that Electronic Warfare (EW) systems play a vital role in warfare: in fighter detection, prevention, deterrence and defeat of attacks by aircraft, UAVs, missiles, radars, maritime vessels, hostile space systems, and cyber threats.

The Global Electronic Warfare Market 2017-2027 is expected to be valued at more than US$ 13 billion in 2017, and will grow at a CAGR of more than 2.6 per cent, exceeding the US's $ 17.5 billion by 2027.[56] Other sources

[53] Wikipedia, "Electronic warfare". https://en.wikipedia.org/wiki/Electronic_warfare
[54] North Atlantic Treaty Organization, "Electronic warfare", last update 16 November, 2011. https://www.nato.int/cps/en/natohq/topics_80906.htm?
See also: Maxim Worcester, "The Evolution of Electronic Warfare", in: International and Regional Security Developments 2018 – Implications for Myanmar, Myanmar: Konrad Adenauer Foundation, 2018, p. 35-38.
[55] Stockholm International Peace Research Institute (SIPRI), "World military expenditure grows to $1.8 trillion in 2018", 29 April 2019. https://www.sipri.org/media/press-release/2019/world-military-expenditure-grows-18-trillion-2018
[56] Business Wire, "Global Electronic Warfare Market 2017-2027 – Research and Markets", Dublin, 10 January, 2018. https://www.businesswire.com/news/home/20180110006076/en/Global-Electronic-Warfare-Market-2017-2027---Research

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

forecast that the electronic warfare market will grow from USD 23.13 billion in 2016 to USS 30.32 billion by 2022.[57] North America will continue to dominate the EW market, followed by the Asia Pacific Region and Europe.

Current trends in the global electronic warfare market include the development of next-generation electronic jammers and the growing demand for intelligence gathering. New concepts and technologies pertaining to cyber and electronic warfare are also being developed.

Electronic Warfare in Action – Some Examples

I would now like to shift attention to the United States of America. According to multiple reports, the Pentagon plans to establish a new task force "to regain U.S. dominance in the electromagnetic spectrum" after US service members experienced Russian jamming tactics. The new task force will produce an "updated electronic warfare strategy and road map" for US Congress under the guidance of Air Force General Paul Selva, vice chairman of the Joint Chiefs of Staff.[58]

After flexing its EW-muscle during the annexation of Crimea following the 2014 Ukrainian revolution, the Russian military ramped up EW testing in war-torn Syria, disabling US communications networks EC-130 aircraft in what the then US Special Operations Command Chief General Raymond Thomas referred to as "the most aggressive EW environment on the planet from our adversaries."[59] These capabilities are now shifting to the Arctic region.

Looking at the US Navy, Lockheed Martin was awarded a $184 Million contract to continue providing the US Navy with SEWIP Block 2 systems with electronic warfare capabilities to existing and new ship combat systems.[60] Furthermore, Lockheed Martin was awarded a $20 million contract for engineering and technical services for the AN/BLQ-10 Electronic Warfare System Technology Insertion. The AN/BLQ-10 submarine electronic warfare system processes radar signals through masts and periscopes to detect threats such as counter detection, collision and target locations. Crews can rapidly analyse and identify critical signals to determine hostile, neutral or friendly situations.[61]

However, Northrop Grumman Aerospace will likewise profit from Navy contracts. The company will start replacing the Navy's ageing EP-3 Aries manned SIGINT propeller plane next year with the MQ-4C long-range unmanned aerial vehicle (UAV) with SIGINT capability. The MQ-4C Triton provides real time intelligence, surveillance, and reconnaissance missions (ISR) over vast ocean and coastal regions. The order amounts to $33.8 million.[62]

---

[57] Markets and Markets Research Private Ltd., Press Release, March 2018.
https://www.marketsandmarkets.com/Market-Reports/electronic-warfare-market-1301.html
[58] The National Interest, "The U.S. Military Is getting Very Serious about Electronic Warfare", June 4, 2019.
https://nationalinterest.org/blog/buzz/us-military-getting-very-serious-about-electronic-warfare-61052
[59] Ibid.
[60] Lockheed Martin News Releases, "Lockheed Martin Awarded $184 Million to Continue Providing the U.S. Navy With Electronic Warfare Systems", 11 February, 2019.
https://news.lockheedmartin.com/2019-02-11-Lockheed-Martin-Awarded-184-Million-to-Continue-Providing-the
[61] Lockheed Martin News Releases, "Lockheed Martin Awarded $20 Million For Engineering and Technical Services for the U.S. Navy's AN/BKQ-10 System", 22 April, 2019.
https://news.lockheedmartin.com/2019-04-22-Lockheed-Martin-Awarded-20-Million-for-Engineering-and-Technical-Services
[62] John Keller, "Northrop Grumman to outfit Navy MQ-4C Triton unmanned aircraft for SIGINT missions in $33.8 million order", in: Military & Aerospace Electronics, 24th July 2019.
https://www.militaryaerospace.com/sensors/article/14036815/sigint-unmanned-triton

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Officials of the Cyber Warfare Detachment of the Naval Air Systems Command in Lakehurst, N.J., issued a broad agency announcement on Monday (N68335-19-R-0370) for resilient cyber warfare technologies used in naval aerial weapons, in view of insufficient cyber research and threat-information for digitally connected weapons.[63]

A brief glance at the US Air Force. In the next decade unmanned combat aircraft could join high-performance US military fighter jets as trusted partners in dogfighting. The F-35 and F-15EX fighter jets may be equipped with drone wingmen in the coming years as Air Force leaders explore ways to team Lockheed Martin's F-35 and Boeing's new F-15EX with the XQ-58 Valkyrie drone or similar unmanned platforms in future dogfighting. The Valkyrie can fly at high subsonic speeds, take off without a runway, and, according to Kratos, meet or exceed the Air Force's requirement for a 1.500 nautical-mile range with a 500-pound payload.[64]

The Air Force is also assessing whether other unmanned aerial systems would complement the Skyborg program. A March request for information describes a "modular, fighter-like aircraft" that is autonomous and attritable, with open systems that allow it to be updated with new Artificial Intelligence (AI) software or new hardware. Desired characteristics include the ability to detect and avoid obstacles and bad weather, and to take off and land autonomously.[65]

Furthermore, the U.S. Army is currently modernizing its electronic warfare capabilities. As the army refines its doctrine, it will need to emphasise coordination between EW and intelligence so as to provide EW crew with essential information required to discern friendly and enemy signals.[66]

It would exceed the scope of this study to further elaborate on developments in electronic warfare in the Asia-Pacific region. I refer here only to *The Military Balance – The Annual Assessment of Global Military Capabilities and Defence Economics*, by the International Institute for Strategic Studies (IISS), London, 2019. I would like, however, to briefly refer to developments in the East and South China Sea.

In the Asia-Pacific Region the East and South China Sea is a hotspot and is set to remain so. On February 16, 2018 I received an email from the Asia Maritime Transparency Initiative (AMT) Center for Strategic and International Studies (CSIS), Washington, that included high-grade photographs of China's seven artificial islands in the Spratly Group in the South China Sea. A few images of the Fiery Cross Reef, the Subi Reef and the Mischief Reef serve as an example of this and highlight electronic warfare capabilities.[67]

Fiery Cross Reef: The images date from November 28, 2017 and depict the northern part of the 3000-meter runway and its large communications and signal intelligence facilities. A tall tower housing a sensor/communi-

[63] John Keller, "Navy asks industry for information technologies for defending aerial weapons against enemy cyberattacks", in: Military & Aerospace Electronics, 9th July 2019.
https://www.militaryaerospace.com/trusted-computing/article/14035892/weapons-cyberattacks-defending
[64] John Keller, "U.S. fighter jets could work together with high-performance unmanned combat aircraft dogfighting by 2020s", in: Military & Aerospace Electronics, 23 May 2019.
https://www.militaryaerospace.com/unmanned/article/14033737/unmanned-fighter-jets-dogfighting
[65] Ibid.
[66] Mark Pomerleau, "How will the Army use electronic warfare? The Pentagon's weapon tester wants to know", in: C4ISR, 4 February 2019.
https://www.c4isrnet.com/electronic-warfare/2019/02/04/how-will-the-army-use-electronic-warfare-the-pentagons-weapon-tester-wants-to-know/
See also: Defense Blog, "U.S. Army modernizes electronic warfare capabilities", 12 February 2019.
https://defence-blog.com/army/u-s-army-modernizes-electronic-warfare-capabilities.html
See also: J.R. Wilson, "Electronic warfare on the ground", in: Military & Aerospace Electronics, 1 February 2019.
https://www.militaryaerospace.com/home/article/16709607/electronic-warfare-on-the-ground
[67] Asia Maritime Transparency Initiative, CSIS Center for Strategic & International Studies,"Comparing Aerial and Satellite Images of China's Spratly Outposts", 16 February 2018.
https://amti.csis.org/comparing-aerial-satellite-images-chinas-spratly-outposts/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

cation facility topped by a radome, and a field of upright poles, most likely a high-frequency radar array is also indicated together with a large communications/sensor array, perhaps serving as a signal intelligence communications hub for Chinese forces in the area.

The Subi Reef: The image refers to a sensor/communications facility topped by a radome and shows a high-frequency array, and, moreover, hardened structures with retractable roofs believed to be shelters for mobile missile launchers.

The Mischief Reef: The image shows a large sensor/communications facility topped by a radome, and details three towers housing sensor/communication facilities topped by radomes.

The images also show details of hangars for China's fighter-jets, bombers and transporters. Shelters for anti-ship cruise missiles, ammunition storage depots, and a range of electronic and signals intelligence equipment including over-the-horizon radars, which can likewise be discerned.

I recall a statement by Chinese President Xi Jinping in 2015, namely, that China had no intention to militarise the artificial islands around the Spratly islands; what we see now, however, is that over 40 different radar facilities represent a significant enhancement of China's C4ISTAR capabilities (command, control, communication, computers, information/intelligence, surveillance, targeting acquisition and reconnaissance).

In my view, the USA is set to remain a major power in international politics and will also continue to cooperate with their allies in the Asia-Pacific region. For us Europeans, it is essential to continue careful observation of events in the South China Sea and neighbouring regions, that we adjust in good time to critical developments and elaborate concomitant political, economic and military strategies.

Finally, I would like to conclude this section by some remarks by our ISPSW Senior Advisor, Maxim Worcester, on the importance of quantum technology, especially since all intelligence services face particular challenges in this area.

Worcester writes: "Quantum technology is set to be a game-changer in EW. Currently, while the US is leading in this field, China is investing heavily therein, both in terms of funding and manpower. The first to master this emerging technology will render most if not all countermeasures obsolete. Communications based on quantum technology are entirely secure and quantum RADAR systems make stealth aircraft visible and thus obsolete. Backed by the Chinese government at the highest level, Chinese scientists are apparently making rapid progress in a variety of different applications, including quantum encryption, which promises uncrackable communication.

China has undertaken a massive national campaign to become world leader in this field. Recently, the Chinese Academy of Sciences has established the Quantum Science and Technology Innovation Research Institute and is planning to establish a national quantum information science laboratory.

In 2016, China launched the world's first quantum satellite, Micius, which could become the first piece of global quantum network for uncrackable communications. The Chinese leadership sees quantum technology as both a means of security and as an enabler in bridging the gap between its military capabilities and those of its potential adversaries.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

There appears no lack of funding for this hugely significant development; on the contrary, China clearly understands that EW is an essential part of power projection and warfare and has also recognized the future of EWs in the development and implementation of quantum technology across the Electromagnetic Spectrum."[68]

The importance of electronic warfare – both active and passive – will continue to increase. We may also assume that nations without electronic warfare capability stand little chance in an open conflict.

Similarly, it stands to reason that defence budgets will of necessity grow in proportion to meeting the costs of expensive and sophisticated weapons systems.

Finally, nations that have so far opted against the use of electronic warfare as an offensive weapon – by using cyber systems, for example – will be obliged to rethink their policy.

A2/AD and Technology

Following an invitation by the German Federal Foreign Office, I had the pleasure of attending the conference *Capturing Technology*. *Rethinking Arms Control* held on 15 March, 2019. In his welcome address, Heiko Mass, Federal Minister for Foreign Affairs, pointed out that "today we are facing a new frontier. In the digital age, technological progress is moving at lightning speed – with unprecedented and far-reaching impacts on the present, but also on future conflicts and warfare. Repeating the mistakes of the past could prove disastrous for humankind. We need to think ahead, and we must start thinking now…

Will we be able to trust autonomous weapon systems to select and attack targets without human involvement? How can we defend our energy supply against malicious use of cyber instruments? Will revolutionary advances in gene editing and synthetic biology make it easier and more attractive for terrorists or states to weaponise biological agents? Can we reduce the risks to strategic stability associated with new missile technology and missile proliferation?

If we do not find answers to these questions, we risk opening Pandora's box. Technologically advanced weapons, operating in undefined grey zones, could further undermine existing international arms control regimes. Once deployed, new military technologies would almost certainly trigger a global arms race – with uncontrollable consequences for human security."[69]

When glancing at the content of the conference reader, which included topics such as *Cyber Instruments and International Security, Weapon Systems with Autonomous Functions, New Developments in Biotechnology, Missile Technology and Challenges Arising from its Proliferation*, *Trends in Missile Technology*,[70] what sprung to my mind was A2/AD and the challenges for intelligence services; for it is such topics as these that should form an integral feature of permanent intelligence requirements.

Allow me to begin by way of a definition: "An area denial weapon or Anti Access/Area Denial (A2/AD) weapon is a device or a strategy used to prevent an adversary from occupying or traversing an area of land, sea or air. The specific method used does not need to be totally effective in preventing passage (indeed, sometimes it is not) so long as it is sufficient to severely restrict, slow down, or endanger the opponent. Some area denial

[68] Maxim Worcester, "The Evolution of Electronic Warfare", in: International and Regional Security Developments 2018 – Implications for Myanmar", Myanmar: Konrad Adenauer Foundation 2018, p. 35-38.
[69] Message from Heiko Maas, Federal Minister for Foreign Affairs, at the conference *Capturing Technology*. *Rethinking Arms Control,* March 15, 2019, Berlin.
[70] German Federal Foreign Office, *Technology. Rethinking Arms Control*, www.rethinkingarmscontrol.de

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

weapons pose long-lasting risks to anyone entering the area, specifically to civilians, and thus are often controversial."[71]

According to international security scholars Stephen Biddle and Ivan Oerlich, China's A2/AD uses "a series of interrelated missile, sensor, guidance, and other technologies designed to deny freedom of movement, to keep any potential adversaries, including the United States, from intervening in a conflict off of China's coast or from attacking the Chinese mainland."[72]

While Gholz advocated a strategy based on restraint, he pointed out that whether or not the United States pursue a restrained grand strategy or a deeply engaged one, having capable allies is preferable. If US allies in East Asia were to adopt an A2/AD strategy, they would be far more capable of protecting themselves than they are now.[73]

Looking at the "Yellow Tiger's" A2/AD capabilities, China has indeed made significant gains in asymmetrical weaponry as a means of blunting America's advantages. A centerpiece of this strategy is an arsenal of high-speed ballistic missiles designed to strike moving ships. The latest version, the DF-2D and, since 2016, the DF-26, are also known as "carrier killers", since they are capable of threatening the most powerful vessels in the American fleet long before they get close to China. These missiles are difficult to detect and intercept and are directed at moving targets by an increasingly sophisticated Chinese network of radar and satellites. The "carrier killers" have been supplemented in 2018 by the deployment of missiles in the South China Sea. The weaponry includes the new YJ-12B anti-ship cruise missile, which puts most of the waters between the Philippines and Vietnam in range.[74] This deployment will challenge and threaten the US navy deployment across Asia and the Pacific.

Of no less interest is a new development of lightweight, remote sensing platforms built by the China Electronics Technology Group Corporation, a state-owned enterprise specializing in-high technology defense and security products – especially sensors, communications, and networking. These mobile and deployable platforms may turn out to be important complements to the network of long-range sensors and arrays that China has already constructed on its major bases in the Spratly Islands.[75]

To counterbalance these threats, analysts think that the US needs greater numbers of long-range, high-capacity launch platforms. On the offensive side, promising new long-range strike weapons include the LRASM anti-ship missile, the stealthy JASSM-ER cruise missile and the army's multi-faceted Long-Range Precision Fire Program. On the defensive side, the army's maneuver short-range air defense program and the Navy's SM-3 and SM-6 offer promising force protection capabilities.[76]

Furthermore, US military strategists must identify key geographic areas designed to challenge China's strategy by improving US strategic depth, diversifying logistical options for regional air refueling and naval weapons

[71] Wikipedia https://en.wikipwdia.org/wiki/Area_denial_weapon
[72] What is A2/AD and Why Does it Matter to the United States?, Charles Koch Institute; https://www.charleskochinstitute.org/event/anti-accessarea-denial-a2ad-U-S-China-relations/
[73] Ibid.
[74] Steven Lee Meyers, "With Ships and Missiles, China Is Ready to Challenge U.S. Navy in Pacific", New York Times, August 30, 2018, https://www.msn.com/en-in/news/world/with-ships-and-missiles-china-is-ready-to-challenge-us-navy-in-pacific/ar-BBMDitt
[75] Steven Stashwick, "China May Deploy New Maritime Surveillance Platforms in South China Sea", The Diplomat, April 3, 2019, https://thediplomat.com/2019/04/china-may-deploy-new-maritime-surveillance-platforms-in-south-china-sea/
[76] Sebastien Roblin, "A2AD: The Phrase That Terrifies the U.S. Military (And China and Russia Loves It)," The National Interest, April 9, 2019, https://nationalinterest.org/blog/buzz/a2ad-phrase-terrifies-us-military-and-china-and-russia-love-it-51597

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

reloading, and strengthening the sea and air defenses of allies and US territory. Manus Island, north of Papua New Guinea, centrally located in a strategic triangle that spans from Guam, westwards to the Philippines, and south to the northern Australian coast, is perfectly situated to support regional refueling operations both in the air and at sea.[77]

It seems to me that Beijing is also very interested to know what's going on near Manus Island: high-tech Chinese ships have been detected near the island as the United States and Australia began naval base upgrades at Lombrum Naval Base. The deployment of Chinese ships to waters near Papua New Guinea has sparked concern as experts believe any information gathered by the Chinese surveys could be crucial in any future maritime conflict with the United States.[78]

Although US President Donald Trump has expressed doubts about NATO's alliance capacity and has also bounced off the US allies in Asia, in my view these states are indispensable for US global strategy.

In 2020, for example, Japan is scheduled to adopt a system that allows its defense forces to simultaneously share information on enemy missiles – such as a missile's location, direction and speed – with the US military, thus enabling the allies to better track and destroy them. Employing Cooperative Engagement Capability (CEC) will link Japanese and US forces more closely and strengthen the alliance. Japan envisions using its ships to intercept missiles headed for US navy vessels, and vice versa.[79] Furthermore, in February 2019 the Japan Maritime Self Defense Forces (JMSDF) commissioned its second Asahi-class guided missile destroyer. The ship is mainly an anti-submarine warfare platform.[80]

In the coming years Japan will also acquire or develop a number of unmanned vehicles for surveillance. The blueprint includes three maritime surveillance drones in the procurement for fiscal years 2019 to 2023, and an eventual 20 of the ship-transportable aerial vehicles. In fiscal year 2021, Japan's Air Self-Defense Forces will deploy the US-made Global Hawk unmanned aerial vehicle, thus creating a special unit to handle the drone which can stay airborne for long periods. Furthermore, the SDF plans to develop an underwater drone for gathering information.[81]

The importance of Japan for US security and other US allies in the Asia-Pacific region is also underlined by Tokyo's intention to purchase 105 new F-35 Lightning II stealth fighter jets from the US, thereby equipping it with the

[77] Jerry Hendrix and Harry Foster, "China has Impressive A2/AD Capabilities, but Smart Positioning Can Let The Navy Avoid them", The National Interest, November 10, 2018, https://nationalinterest.org/blog/buzz/china-has-impressive-a2ad-capabilities-smart-positioning-can-let-navy-avoid-them-35702
[78] Imogen Reid, "China Boosts Surveillance as US and Australia Naval Base Upgrades Begin", New Zealand Herald, April 21, 2019, https://www.news.com.au/technology/innovation/military/china-boosts-surveillance-as-us-and-australian-naval-base-upgrades-begin/news-story/2f1cfb7623f98eefe640bbdce3b4ccbd
[79] Masaya Kato, "Japan and US to Sharpen Missile Defense with Real-time Data Sharing", Nikkei Asian Review, 25 August, 2018, https://asia.nikkei.com/Politics/International-relations/Japan-and-US-to-sharpen-missile-defense-with-real-time-data-sharing
[80] Franz-Stefan Gady, "Japan Commissioned New Anti-Submarine Warfare Destroyer", The Diplomat, 6 March, 2019, https://thediplomat.com/2019/03/japan-commissions-new-anti-submarine-warfare-destroyer/
[81] Masaya Kato, "Japan steps up deployment of defence AI and robots", Nikkei Asian Review, 27 January, 2019, https://asia.nikkei.com/Politics/Japan-steps-up-deployment-of-defense-AI-and-robots
Regarding China's High Tech Ambitions see: Sophie-Charlotte Fischer, "Artificial Intelligence: China's High-Tech Ambitions", Center for Security Studies (CSS), ETH Zürich, 8 February, 2018, https://css.ethz.ch/en/center/CSS-news/2018/02/artificial-intelligence-chinas-high-tech-ambitions.html
See also: Tetsuro Kosaka, "AI Arms Race Risks Rise of Uncontrollable Killer Robots", Nikkei Asian Review, May 12, 2019, https://asia.nikkei.com/Spotlight/Comment/AI-arms-race-risks-rise-of-uncontrollable-killer-robots
See also: Kai-Fu Lee: "AI Superpowers: China, Silicon Valley, and the New World Order", Boston: Houghton Mifflin Harcourt, 2018.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

largest F-35 fleet of any US ally.[82] And on Tuesday, 17 September, 2019, Lockheed Martin announced, that the company has continued development on its Advanced Electro-Optical Targeting System (EOTS) used in the F-35 Lightning II. The system includes a larger aperture and provides pilots with multi-spectral sensing options such as high-resolution Mid-Wave IR, Short-Wave IR and Near IR.[83]

Military experts believe that Japan's planned purchase of 147 F-35 planes (105 F-35As, 42 F-35Bs) at a price of US$ 89.2 – US$ 115.5 million per plane equipped with cutting-edge technology, will not only dominate the South China Sea, but that it is also destined to become the preeminent air force in Asia, second to the United States. Japan's sizeable F-35 acquisition makes it one of the few nations capable of networked warfare in the region. This will also accelerate the arms race in Asia, with China, Australia, South Korea and Singapore, all of which are bulking up their military might with the acquisition of state-of-the-art stealth fighters.[84]

In this environment, intelligence collection, intelligence analysis and cooperation with partner services is indispensable. Accordingly, the German Federal Intelligence Service (BND) cooperates with 450 partner services in 160 countries.

It is regrettable that South Korea announced on 20 August 2019 that it will scrap the intelligence sharing agreement, known as the General Security of Military Information Agreement (GSOMIA) with Japan. Withdrawing from the intelligence sharing agreement means that Seoul will no longer receive quick notification on irregular activities in regional waters, namely, in what Japan calls the Sea of Japan, and South Korea the East Sea.[85]

The pact, scheduled to expire in November 2019, offers many benefits to South Korea, complementing its military weak points. Seoul can view up-to-date images from Japanese satellites, as well take advantage of exceptional monitoring and detection capabilities of Japanese anti-submarine patrol aircraft. On the other hand, Japan will receive missile information from South Korean radar sites and reconnaissance aircraft. This allows Tokyo to rapidly determine a projectile's launch site and flight pass, thus enabling valuable analysis before missiles can reach the Japanese archipelago.[86]

The US have expressed disappointment as they were not informed in advance, and Secretary of State Mike Pompeo remarked: "We are disappointed to see the decision the South Koreans made about that information-sharing agreement. We're urging each of the two countries to continue to engage. There is no doubt that the shared interests of Japan and South Korea are important and they're important to the United State of America."[87]

---

[82] "Trump Announces Japan's Purchase of 105 New F-35 Stealth Aircraft", Defense Blog, 27 May, 2019, https://defence-blog.com/news/trump-announces-japans-purchase-of-105-new-f-35-stealth-aircraft.html
[83] "Lockheed Martin develops advanced targeting system for F-35", Defence Blog, 18 September, 2019, https://defence-blog.com/news/lockheed-martin-develops-advanced-targeting-system-for-f-35.html
[84] Wilson Wong, "Japan's F-35 Acquisition and the Arms Race in the Western Pacific: Strategic Game Changer or Epic Boondoggle?", The Asia Pacific Journal, Volume 17, 1 June, 2019, https://apjjf.org/2019/11/Wong.html
[85] Grace Shao, "South Korea is Scrapping a Security Deal with Japan – Here's Why it Matters", CNBC, 23 August, 2019, https://www.msn.com/en-ph/news/world/south-korea-is-scrapping-a-security-deal-with-japan-%E2%80%94-heres-why-it-matters/ar-AAGdXi0
[86] "Seoul's pullout from intelligence pact sows seeds of instability", Nikkei Asian Review Editorial, 2-8 September, 2019, p 52.
[87] Hyonhee Shin, Josh Smith, Kiyoshi Takenaka, "South Korea to Scrap Intelligence-sharing Pact with Japan Amid Dispute over History", Reuters, 22 August, 2019, https://www.reuters.com/article/us-southkorea-japan-labourers/south-korea-to-scrap-intelligence-sharing-pact-with-japan-amid-dispute-over-history-idUSKCN1VC0WR
See also: Michael R. Gordon, "South Korea Withdrawal From Intelligence Pact With Japan Caught U.S. by Surprise, Top Official Says", The Wall Street Journal, 28 August, 2019, https://www.wsj.com/articles/south-korea-withdrawal-from-intelligence-pact-with-japan-caught-u-s-by-surprise-top-official-says-11567024514

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The Japanese are still interested in cooperating closely with South Korea. Thus, as Japanese Chief Cabinet Secretary Yoshihide Suga remarked, "We want to continue cooperating fully, including on exchanging information. The framework will remain in effect until 22 November, 2019. We want to deal with the situation appropriately as long as the agreement is alive."[88] But Japan is already eager to prove to the international community that should the agreement not be prolonged, the effect will be minimal. Most likely as part of this effort, Japan's Defense Ministry has released data that it collected on eighteen missiles North Korea tested on nine separate occasions since May of this year.

I shall conclude this section of my study by taking a look at space. China has successfully launched its first rocket into space from a mobile platform in the Yellow Sea on 5 June, 2019, and placed seven satellites on their planed orbit. The launched satellites included those for weather forecasting and ship-navigation systems. The launch was conducted by the state-run company China Aerospace Science and Technology. China's neighbors are concerned that the technology could be used for military purposes.[89]

I would like to quote Ralph Thiele, President of EuroDefense Germany, in this connection, when he referred to the vital importance of unhindered access and freedom to operate in space. He writes: "Satellite Communications (SATCOM) can be expected to be the crucial backbone of evolving communications network. As access to space becomes cheaper, satellites are becoming mass-production devices. The unhindered access to and freedom to operate in space, is of vital importance to nations and international organizations, such as NATO and the European Union. Navigation and weather monitoring, communications and financial networks, military and intelligence systems – all of these and more have components in the space domain.

Opponents understand this well and have been preparing hybrid measures for downgrading C4I. Cyber threats to space systems by state/non state actors are rapidly developing. Consequently, the tasks involved in securing outer space and cyberspace are converging. There is a premium on disruptive and game-changing technologies that are autonomous, reconfigurable, agile and adaptable. Governments, commercial customers and industry should all prepare themselves for new business models and new economics of space since there are substantial changes on the horizon. Cyber is the driver."[90]

Recommendations

1. As the crisis potentials described in the threat situation continue, foreign and domestic intelligence services are presented with specific challenges. Although the Federal Government has established thousands of new positions and financial resources for the relevant services, staffing requirements will only be achieved gradually. Suitable personnel must first be identified, recruited and trained.

   To cope with the interim period, it would advisable to extend retirement age by several years – with employees' consent – or to hire retired employees. Some foreign and domestic intelligence services have been very successful, especially when drawing on existing employees' many years operational expertise.

[88] Rieko Miki, "What Intel Pact? Japan Flaunts North Korea Missile Analysis", Nikkei Asia Review, 11 September, 2019, https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/What-intel-pact-Japan-flaunts-North-Korea-missile-analysis
[89] Shunsuke Tabeta, "China Launches Rocket from Sea as Tensions with US Grow", Nikkei Asian Review, 6 June, 2019, https://asia.nikkei.com/Politics/China-launches-rocket-from-sea-as-tensions-with-US-grow
[90] Ralph D. Thiele, "Game Changer 'Cyber' – Towards New Economics of Space? ", in: Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), Issue No. 626, June 2019, Berlin, https://www.ispsw.com/wp-content/uploads/2019/06/626_Thiele.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The geopolitical rise of the People's Republic of China and the shifting of the international balance of power from the standpoint of politics, economics and the armed forces from West to East, should result in Western intelligence services' ability to account for these developments in intelligence-gathering and analysis.

Since NATO is not only a military but also a political organization, it should pay more attention to developments in the Asia-Pacific region. The EU must reorganize itself such as to be adaptable to effective common foreign policy.

As far as intelligence-gathering in the Middle Kingdom is concerned, this is of strategic interest to Germany and Europe in all areas: politics, economics, science, military, technology. Here it is necessary to build first-class sources – so-called inside agents which, though requiring time and patience, can prove particularly effective.

2. The Federal Republic of Germany and the EU will continue to be the focus of Chinese intelligence services. Economics, science, technology and the military are among the focal points of Chinese intelligence-gathering.

   There is also a tangible shift in intelligence-gathering towards political intelligence-gathering, such as gaining knowledge of supranational institutions like the EU or international conferences (G20 summit).

   Furthermore, political positions concerning territorial disputes in the South China Sea or the trade dispute with the US, for example, are of great interest to Beijing and essential to strategic decision-making.

   Other intelligence services operating in the Federal Republic of Germany include the Russian Federation, Turkey, Syria, Vietnam etc. Based on the threat situation, the Federal Office for the Protection of the Constitution (BfV) must be organised such as to ensure 360-degree visibility. The same also applies to the activities of Western intelligence services, which operate in the Federal Republic of Germany – as has been pointed out by the media.

   A common policy should be developed with regard to Huawei's involvement in the development of the 5G network in Germany or the EU, a policy that accounts for security and political aspects.

3. The threat of international terrorism remains, and the cooperation of German services with those of the US is indispensable. In the fight against international terrorism, the EU's Intelligence Analysis Center (INTCEN) is also important. The EU INTCEN has proven its outstanding capabilities in recent years, and thus dealing with cyber threats and fake news makes sense.

   Since the Federal Government attaches greater importance to dealing with right-wing extremism, domestic and foreign intelligence services and other security agencies are required. Again, the challenge is to be able to provide suitable staff. The restructuring of the Federal Office for the Protection of the Constitution (BfV), the Federal Foreign Intelligence Service (BND) and the German Federal Office for Military Counterintelligence Service (BAMAD) is under way. The BAMAD will also be increasingly active in the field of operations, which is highly recommended.

   However, this will only be successful if the BAMAD disposes over a sufficiently large number of recruiters/case officers.

4. The diversity of signals within the electromagnetic spectrum, the reallocation of signals, and sharing between commercial and military spheres has presented a myriad of technological hurdles for engineers to

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

overcome. Maintaining the technological edge, orchestrating cooperation between commercial and governmental sectors, and protecting intellectual properties will be key challenges, where the intelligence community has an important supportive function.

The closing decades of the last century saw the worldwide rise of electronics and software, together with their evolution, penetrating to the heart of military capabilities at all levels, in all domains, and across all services. This created a modern and very complex battlespace. Meanwhile, Electronic Warfare (EW), i.e. action involving offensive or defensive use of the electromagnetic spectrum (EMS), was also growing in prominence across the armed forces. Disruptive technologies have created threats and opportunities that are completely changing and challenging the way that we have conducted EW in the past.

Electronic Warfare has been an afterthought for a quarter of a century, but the exponential growth of space and cyber technologies that rely, above all, on electromagnetic signals has brought about a renewed sense of urgency with respect to rebuilding and recapitalizing EW capabilities, both offensive and defensive. However, due to the increasing dependencies of modern military systems upon the EMS, it is imperative that commanders understand the following:

The modern challenges in dealing with the high-end capabilities of opponents, especially in confrontations requiring operations in Anti-Access/Area Denial (A2/AD) environments, have brought EW back to the forefront. This applies, in particular, to hybrid challenges that emphasize ambiguity.

EU and NATO nations would be well-advised to re-invest in modern EW capabilities so as to build their sufficient capacity for meeting the respective challenges. Intelligence should support situational awareness about upcoming technologies, capabilities and challenges.

5. Anti-access (A2) and area denial (AD) challenges are important to consider. They are imminent in several regions. Opponents can attack NATO, the EU and its member states in all five key domains—air, sea, land, space, and cyberspace.

   While the focus of high-level discussions is predominantly on sophisticated, longer-range adversary capabilities and methods – such as ballistic missiles, submarines, weapons of mass destruction, and offensive space and cyberspace assets – dangerous, though no less technical methods, may include terrorism, proxy warfare or weaponized social media employed by opponents for opening alternative “hybrid fronts”.

   To date, one critical gap has been the significant consideration of A2/AD challenges emerging largely from outside the realm of traditional military competition and violence. When opponents effectively combine political, economic, and informational tools with important military capabilities, the A2/AD challenge becomes more acute and potent. When targeted specifically at NATO and EU vulnerabilities, this may induce “warlike” effects on core own values and interests, while precluding the use of military power as a legitimate response.

   Revolutions in information; personal computing, communications, networking and hybrid forms of warfare – when combined with the proliferation of precision weapons and improvised battlefield lethality – substantially widen the universe of effective A2/AD opponents by individuals and loosely organized groups to sophisticated regional powers. Similarly, the networked mobilization of foreign popular, nonviolent resistance may also prove a significant challenge to freedom of action in the future.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Consequently, breaking down the A2/AD challenge from the intelligence side into respective angles so as to include the hybrid spectrum is recommended.

***

Remarks: The opinions expressed in this contribution are those of the author.

This analysis is an inspiration paper for the study *Hybrid Warfare: Future and Technologies*, Hybrid CoE, The European Centre of Excellence for Countering Hybrid Threats COI Strategy & Defence, Helsinki, in cooperation with StratByrd Consulting, Germany (December 2019). See also: Hybrid Warfare: Challenges for Intelligence Services, Interview Ralph D. Thiele with Dr Peter Roell, in: *Denkwürdigkeiten*, Journal der Politisch-Militärischen Gesellschaft e.V. (pmg), no. 114, December 2019.

About the Author

Dr Peter Roell has been President of the Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) in Berlin since January 2006. His former post was as Senior Advisor for Foreign and Security Policy at the Permanent Representation of the Federal Republic of Germany to the EU in Brussels. While in Germany, he served the German Government as Director of the Asia-Pacific, Latin America and Africa (Sub-Sahara) Department and at German embassies in the Near and Middle East, and in Asia.

Dr Roell studied sinology and political sciences at the universities of Bonn, Taipei and Heidelberg. He gained his Ph.D. from the Ruprecht-Karls-University, Heidelberg.

Dr Roell is an Ancien of the NATO Defence College in Rome and the Federal Academy for Security Policy (BAKS) in Berlin.

Dr Peter Roell

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de