The Importance of Electronic Warfare in a Disrupted World

Dr. Peter Roell

July 2018

Abstract

In his analysis the author focuses on the growing importance of electronic warfare (EW) in a disrupted world, and the growing global electronic market. Furthermore, he gives several examples of electronic warfare in action, and concludes with some remarks on cyber espionage in Germany and the German defence industry.

About 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.

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW

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

The Disrupted World and the Growing Importance of Electronic Warfare

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.

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.

So how does Jim Mattis, United States Secretary of Defense, analyse the present disruptions? In January this year a close acquaintance 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's physical caliphate, threats to stability remain as terrorist groups with long reach continue to murder the innocent and threaten peace more broadly."

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.

Meanwhile, on 29 June, US Intelligence officials declared that in recent months the DPRK has increased development of fuel for nuclear weapons at multiple secret sites.

Furthermore, a brief glance at the global military spending at $ 1.7 trillion underlines the critical situation currently experienced in many regions of the world. China, the second largest spender in global comparison, increased its military spending by 5.6 per cent to $228 billion in 2017. India invested $63.9 billion in military spending in 2017, an increase of 5.5 per cent compared with its budget in 2016, while South Korea's spending rose to $39.2 billion between 2016 and 2017, representing a 1.7 per cent increase.

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW
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

Russia's military spending reached $66.3 billion in 2017, 20 per cent below that of 2016, perhaps due to economic problems. In Central and Western Europe, in 2017, military spending increased by 12 and 1.7 per cent respectively. Total military spending by all 29 NATO members was $900 billion in 2017.

In the Middle East, military expenditure rose by 6.2 per cent in 2017, and Saudi Arabia increased its military spending by 9.2 per cent, reaching $69.4 billion, the third highest military spending in the world. Iran 19 per cent and Iraq 22 per cent both increased their military spending significantly.

The United States continues to have the highest military expenditure in the world. In 2017 the USA spent more on its military than the other seven highest spending countries combined, reaching $610 billion. In addition, the US Congress decided in March this year that military expenditure should be increased to $700 billion this year.

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 necessity for dealing with peer adversaries capable of entering Anti-Access/Area Denial (A2AD) environments, is critical, and the reason for substantial investments in Electronic Warfare capabilities.

The estimated growth of the global electronic warfare market shows an increase of USD 23.13 billion in 2016, to USD 30.32 billion by 2022. Other sources indicate that in 2017 the electronic warfare market is in excess of USD 13 billion, and is set to reach USD 17.5 billion by 2027. North America is forecast to dominate the EW market, followed by the Asia Pacific Region and Europe.

Whatever the case may be, Goldman Sachs stated in its November 2017 report on Japanese equity strategy that it will continue to pay attention to defence stocks in 2018, and has identified those defence manufacturers with lucrative government contracts most likely to grow in the medium- to long-term.

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 a statement by Lockheed Martin on February 8, 2018, the US Air Force declared that its subsonic, turbofan-powered AGM-158 Joint Air-to-Surface Standoff Missile- Extended Range (JASSM-ER) has achieved full operational capability (FOC), and will be installed on the Boeing F-15E Strike Eagle multirole strike fighter.

As of spring this year, the USAF has been operating 219 F-15E Strike Eagles, and the US military plans to purchase over 2.400 JASSMs and 2.978 JASSAM-ERs. The cost per missile amounts to about USD 1 million for the former and USD 1.75 million for the latter. Both cruise missiles are long-range, stand-off radar-evading weapons designed to destroy hostile air defences and well-defended fixed and relocatable targets, and are capable of keeping strike aircraft safely out of range of enemy air defence systems.

The U.S. Air Force and U.S. defence contractor Lockheed Martin successfully tested two long-range anti-ship missiles (LRASM) fired from a B-1B long-range strategic bomber on December 2017. The LRASM is a next

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW
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

generation anti-ship missile with standoff capabilities, designed to detect and destroy specific targets within groups of surface warships.

In the Far East, however, U.S. ally Japan is presently seeking funding for long range cruise missiles for its fighter jets. The missiles in question are the JSM, manufactured by Norway's Kongsberg Defence & Aerospace, and with a range of approx. 500 kilometres, and the JASSM-ER and LRASM missiles, manufactured by the Lockheed Martin Corporation, each with an approximate range of 900 Km.

The missiles are used to defend the Maritime Self-Defence Forces destroyers equipped with the Aegis missile defence system; they may also be used for island defence to repel enemy surface forces or landing forces before they get close.

Japan also plans to deploy electronic-warfare aircraft capable of remote neutralization of enemy air defence and command systems. Tokyo is currently exploring various other options, including Boeing's EA-18G fighter jets, which emit radio pulses for jamming radar and communication systems. The EA-18 G jet is also capable of carrying missiles to knock out radar facilities.

The jets would also enhance Japan's so-called Anti-Access/Area Denial strategy, designed to keep Chinese aircraft and military vessels from encroaching Japanese territory. China is deploying its own electronic warfare aircraft under the military's Strategic Support Forces.

Lockheed Martin has also approached Japan with plans for a next-generation fighter jet based on its elite F-22 stealth fighter, thus demonstrating both Washington's trust in Tokyo as a defence partner and its eagerness to balance the scale on trade with expensive equipment.

At this point, I would also like to draw attention to an incident occurring on January 10, 2018: after spotting a submarine cruising underwater in a north-westerly direction, a Japanese Maritime Self Defence Force P-3C patrol plane dropped a sonar buoy into waters off the Miyako islands in Okinawa Prefecture. The device detected the sound of the submarine's engine, and the MSDF destroyer Onami began tailing it. On January 12, it was confirmed that the vessel belonged to the Chinese Navy. In brief, the MSDF warned the submarine to discontinue its route towards the Senkaku Islands in the contiguous zone. A few hours lapsed: sailing under the Chinese flag, two Chinese ships and the submarine, identified as a Shang-class nuclear-powered attack submarine, were spotted when resurfacing in the East China Sea on January 12.

In my view, this incident shows both that Chinese submarines are not as silent as they should be, and that Japanese MSDF demonstrated their capabilities. Needless to say, this incident will be the subject of extensive discussions in Chinese Naval circles.

Before moving on from Japan, I would like to point out that on January 26, 2018 Japan deployed its first F-35A stealth fighter jet at Misawa Air Base. The F-35A is armed with advanced radar-evasion capabilities and upgraded missile sensors. The fleet is scheduled to expand to 42 jets.

The Japanese Government is also considering procuring short take-off and vertical landing aircraft F-35B stealth planes, and converting the Izumo helicopter carrier into a base for other airpower facilities, suitable, among other things, for fighter jets. The use of F-35B fighters at sea would significantly improve Japan's operational flexibility.

Similarly, South Korea is currently negotiating the purchase of 20 additional F-35A Stealth fighter jets for boosting the Republic's precision strike capability against North Korea missile and command and control

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW
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

targets in the event of a full-scale war on the Korean Peninsula. The ROK Air Force plans to initiate deployment of the First F-35As in 2018, whereby delivery of all 40 aircraft is scheduled for 2021.

In addition to its 180 cruise missiles, South Korea revealed in February 2018 that the country has concluded a contract for 90 German-built Taurus KEPD 350 long-range, precision-guided cruise missiles. The cruise missile has a range of 500 Km and is capable of flying at extremely low altitudes. It is also equipped with a jam-preventing GPS system and is to be integrated into to the ROK Air Force F-15K.

In the Asia-Pacific Region the East and South China Sea is a hot spot, 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, showing 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 the electronic warfare capabilities.

Fiery Cross Reef: The images date from November 28, 2017; they show the northern part of the 3000-meter runway and its large communications and signal intelligence facilities. Furthermore, a tall tower housing a sensor/communication facility topped by a radome, and a field of upright poles, most likely a high frequency radar array; and 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 of 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 can also be discerned.

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

In my view, the USA will 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.

Cyber Espionage

I have covered, in brief, Germany, the USA, Japan, South Korea and the state of affairs in the South China Sea. In returning to Germany, I would now like to conclude by turning to the question of cyber espionage in my country, and to the German defence industry.

In December 2017, the German Federal Office for the Protection of the Constitution (BfV), Germany's Domestic Intelligence Service, issued a public warning that an Asian Intelligence Service has created thousands

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW
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

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 an Asian intelligence service masquerading as employees of headhunting agencies, consulting firms, think-tanks or as scientists.

Recruitment targets were mainly 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 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 very plausible – given the importance attached to keeping face in Asia – that the government of this Asian 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 did not lead to the 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 as in the economy, industry and the military – this could result in enormous damage to the Federal Republic of Germany.

Remarks on the German Defence Industry

I conclude this analysis with a few words on the German Defence Industry. Germany, a major economic power in Europe, has outlined plans to increase its defence expenditure in the period 2017-2022 in its attempt to strengthen the combat readiness of the Country's armed forces. Estimates of German defence expenditure indicate that it is set to increase at a Compound Annual Growth Rate (CAGR) of 5% between 2018-2022, compared to a CAGR of 2.8% over the period between 2013 and 2017.

The German Ministry of Defence plans to spend billions of Euros on armaments this year to tackle deficiencies in armed forces' equipment. In April 2018, newspapers reported that Germany's Defence Minister, Dr. Ursula von der Leyen, has submitted a list to the parliament's budget committee comprising eighteen major procurement projects, each of which is worth over 25 million euros.

Orders include procuring Israeli Heron TP drones, seven rescue helicopters, six Lockheed Martin Corp's 130J Hercules transport aircraft. Several improvements to Puma armed personnel carriers, a maintenance contract for NH90 helicopters, radar technology for Eurofighter, telecommunication facilities for frigates, and new combat uniforms and protective equipment are also included.

In 2017, the German defence budget, which includes military pensions, amounted to US$ 41.7 bn.

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW
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

Below are three examples of products manufactured by German Industry, the German Corporation DIEHL.

The first slide shows the PARS 3 LR Precision Standoff Missile System, the primary armament for the German Tiger helicopter. It is supplied by the PARSYS GmbH, a joint venture of Diehl and MBDA Deutschland.

photo: DIEHL

The second slide shows the RBS15 Mk3, a long-range, all-weather-capable, fire-and-forget missile, remarkable for its high manoeuvrability enabling it to fly at extremely low altitudes above the water's surface, or around and over islands at distances considerably greater than 200 km.
The weapon is extremely resistant to electronic countermeasures, is characteristically extremely robust in repelling responses by air defence sites that dispose over guided-and tube weapons. Diehl Defence supplies the RBS 15 Mk3 heavy anti-ship missile as the primary weapon for the German Navy's new K130 corvette. A special feature of the ultra-modern German-Swedish missile is its additional precision capability in engaging land targets.

photo: DIEHL

Slide 3 shows the passive Ship Infrared Monitoring and Observation Equipment SIMONE. The system is optimized for early detection of threats to vessels when faced with pirate and terrorist attacks. The system's strengths come into play during port calls and coastal operations, where attacks may be carried out from land or sea. In such scenarios, conventional radar systems quickly reach their limits.

photo: DIEHL

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW
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

Conclusion

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 have to grow in proportion to the necessity of meeting the costs of expensive and sophisticated weapon 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.

***

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

About the Author of this Issue

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

© Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW

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