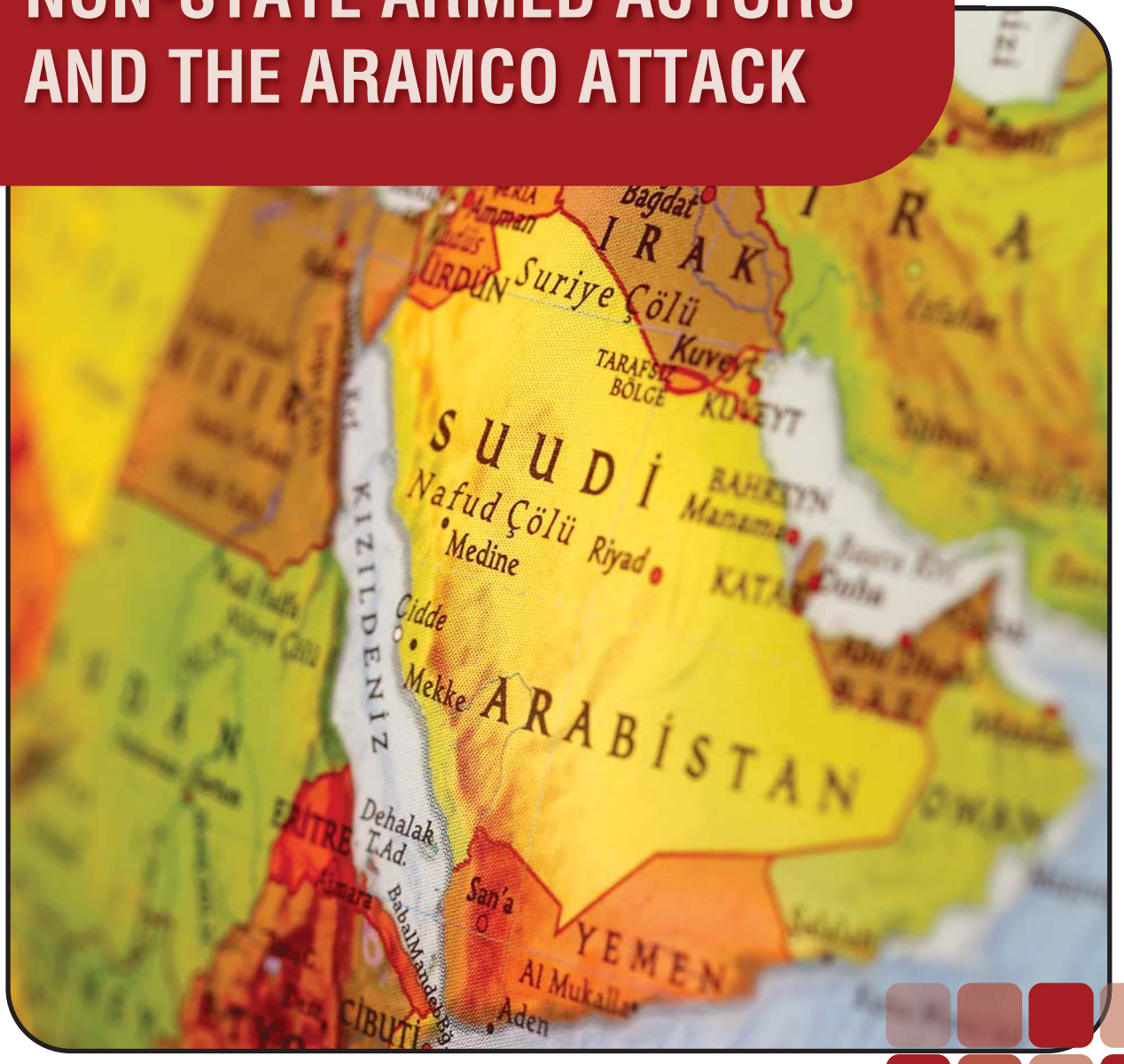
Ortadoğu Araştırmaları Merkezi
مركز دراسات الشرق الأوسط
Center for Middle Eastern Studies
ORSAM

Analysis
No: 234 /October 2019

CRITICAL INFRASTRUCTURES, NON-STATE ARMED ACTORS AND THE ARAMCO ATTACK



ASST. PROF. GÖKTUĞ SÖNMEZ,
GÖKHAN ERELİ

Copyright

Ankara - TURKEY ORSAM © 2019

Content of this publication is copyrighted to ORSAM. Except reasonable and partial quotation and use under the Act No. 5846, Law on Intellectual and Artistic Works, via proper citation, the content may not be used or re-published without prior permission by ORSAM. The views expressed in this publication reflect only the opinions of its authors and do not represent the institutional opinion of ORSAM.

ISBN: 978-605-69731-0-9

Center for Middle Eastern Studies
Adress : Mustafa Kemal Mah. 2128 Sk. No: 3 Çankaya, ANKARA
Phone: +90 850 888 15 20 Faks: +90 (312) 430 39 48
Email: orsam@orsam.org.tr
Photos: Anadolu Agency (AA)

Ortadoğu Araştırmaları Merkezi
ORSAM مركز دراسات الشرق الأوسط
Center for Middle Eastern Studies

ANALYSIS

CRITICAL INFRASTRUCTURES, NON-STATE ARMED ACTORS AND THE ARAMCO ATTACK

About the Authors

Asst. Prof. Göktuğ Sönmez

Received his bachelor's degree in International Relations from Bilkent University, his master's degree in International Relations at London School of Economic (LSE), and his PhD from the School of Oriental and African Studies (SOAS), University of London. His research areas are International Relations Theory, Turkish Foreign Policy, and Radicalization and Violent Extremism. He conducted research on these areas at several think-tanks including the Center for Strategic Research of the Ministry of Foreign Affairs of the Republic of Turkey, Global Strategy Institute and the ORSAM. He currently works as the Director of Security Studies at ORSAM.

Gökhan Ereli

Was born in Ankara in 1992. He graduated from Kırıkkale University, International Relations department with the highest CGPA in his graduating class. Upon graduating, he enrolled in Middle East Technical University (METU) International Relations Master's with thesis program in 2015. He earned his Master's degree with the thesis "The Impact of American Exceptionalism on U.S. Foreign Policy". Currently, he continues his studies at Middle East Technical University (METU), International Relations Ph.D. program. Also, he is working as a research assistant within the body of ORSAM, Gulf Studies. While his main area of interest is the Gulf region and American foreign policy, his special area of interest is the foreign policies of the United Arab Emirates and Qatar. He speaks advanced English and simple Arabic.

October 2019

Table Of Contents

Introduction:

The Definition And Evolution Of Critical Infrastructures

With respect to the concept and definition of the very term "critical infrastructure", several different definitions and components of critical infrastructures can be found in official documents and statements while many common features and characteristics can also be found. For instance, the UN Security Council, in 2017, adopted the resolution 2341, titled Protection of Critical Infrastructures and Enhancement of States' Capacities to Prevent Attacks against Critical Infrastructures, focusing on the threat of terrorist attacks against national and international critical infrastructures and urges the Member States to take necessary measures to prevent such terrorist attacks. In the UN OCT and UN CTED joint report, the critical infrastructures, as the Chair of CTITF Working Group on "Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security", INTERPOL refers to the very concept of "critical infrastructure" as the "life support system of our everyday existence, and make no distinction between cyber and physical critical infrastructures.[i]

In accordance with the UNSC Resolution 2341, preparedness for such attacks includes "prevention, protection, mitigation, response and recovery" "with an emphasis on promoting security and resilience of critical structure" and protective measures include "public information and warning, operational coordination, intelligence and information sharing, interdiction and disruption, screening and risk management so on and so forth.[ii] Water infrastructures, transportation infrastructure and energy infrastructure is among the ones referred to the UNOCT, UN CTED and INTERPOL joint report and several examples such as the Brussels attack of ISIS to airport and underground, Al-Qaida attacks on oil facilities and personnel in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen, and ISIS' around 20 major attacks in Syria and Iraq only between 2013 and 2015 on water infrastructure are also mentioned.[iii] In terms of the cyber environment, manipulation of systems and data, shutting down crucial systems and limiting access to crucial systems or information via cyber-attacks[iv] are also a key aspect of the threat against critical infrastructures which would have serious impact on banking systems, information sharing, satellite systems and more.

The US Department of Homeland Security, defines the concept as a sector "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety or any combinate, on thereof. In a more detailed overview of the components of critical infrastructure (CI) in line with the Presidential Policy Directive 21 (PPD-21) it refers to 16 key components of critical infrastructure, namely Chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defence industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear reactors, materials and waste sector, transportation systems sector, water and wastewater systems sector.[v]

The UK's Centre for the Protection of National Infrastructure as one of the key actors in advising the government regarding security-related issues concerning the UK national infrastructure and directly accountable to the Director General of MI5, refers to critical infrastructures as "facilities, systems, sites, information, people, networks and processes, necessary for a country to function

and upon which daily life depends. It also includers some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public" such as civil nuclear and chemical sites. CPNI lists 13 key CI (the UK version is CNI due to the choice of Critical National Infrastructure) sectors including chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water in addition to some sub-sectors such as police, ambulance, fire services and coast guard which fall under the main sector "emergency services". National Cyber Security Centre (NCSC) is responsible for the cyber protection, thus, making the two institutions combined as the key defence line against terrorist threat on Cis. [vi] House of Commons' definition, in addition, is as follows:

'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state.' [vii]

The 2017 report of the Joint Committee on the National Security Strategy, "Cyber Security of the UK's Critical National Infrastructure", refers to 2017 WannaTry attack which had a major impact on National Health Service (NHS) system for several days as a main example of such efforts along with the Russian cyber-espionage and attacks on energy infrastructure such as the ones "affected Ukraine's energy grid in 2015 and 2016."[viii]

> Based upon above mentioned definitions and references to the key components of CI, it can be argued that CI broadly refers to the systems and services as well as the people that have a direct impact on everyday life of citizens, security mechanism of the state apparatus, and economic functioning of the main institutions which would in turn damage the overall functioning of a state and society.

The European Union's definition for the term CI is "an asset or system which is essential for the maintenance of vital societal functions. The damage to critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, may have a significant negative impact for the security of the EU and the well-being of its citizens". The European Programme for Critical Infrastructure Protection (EPCIP), European Programme for Critical Infrastructure Protection Communication of 2006Directive on European Critical Infrastructures of 2008, Critical Infrastructure Warning Information Network (CIWIN) and European Reference Network for Critical Infrastructure Protection (ERN-CIP) are some of the key tools at the EU's disposal in order to address the issue[ix], showing the significance given to the concept as well as to the preparedness

level and protection of Member States in the face of a possible terror attack against CIs.

Based upon above mentioned definitions and references to the key components of CI, it can be argued that CI broadly refers to the systems and services as well as the people (which is only mentioned by the UK's definition but stand out as another key component due to the possible attacks on the people who run, monitor or coordinate the functioning of key critical infrastructures) that have a direct impact on everyday life of citizens, security mechanism of the state apparatus, and economic functioning of the main institutions which would in turn damage the overall functioning of a state and society.

A Brief Overview of Some Recent Attacks against CIs

Even though historically, the widely used tactics during times of crisis and/or war such as attacking water and food supply lines, fields, people carrying strategic information, manufacturing systems and sabotages against weapon and ammunition production lines can be seen as the early predecessors of attacks against critical infrastructures, each and every innovation and discovery in the field of economics, security and politics brought new tools, institutions, staff, and resources that can be under attack from various aggressors. With the advances in defence industry and military technology, capabilities of both defending these as well as attacking them witnessed a dramatic rise for both states and non-state armed actors.

Some of the recent most sensational and well-known attacks by not only terrorist groups but also non-state armed actors as well as criminal groups show the growing threat of attacks on critical infrastructures. For instance the 2006 jamming of the Thuraya mobile satellites from various locations in Libya, Tamil Tigers' hijacking of an Intelsat transponder to disseminate their message and Falun Gong's disruption of satellite broadcast in 2004, SCADA cyber-attack on the Ukraine energy grid, cyber-attack on the core command-and-control system of Rye Brook,

New York Dam in 2013, North Korean hackers' SWIFT attacks in 2015 and 2016, cyber-attack against the Wolf Creek Nuclear Operation Corporation in Kansas.[x] Burjesia attack in June 2019 targeting the site where ExxonMobil, Shell and ENI headquarters, PKK's 2016 attack on the Kirkuk-Ceylan oil pipeline targeting almost 66 kms of the pipeline, causing disruption in the oil flow and attempted attack on the same oil pipeline passing through Mardin in 2015 within a long list of attacks carried out by the group against the same oil pipeline quite frequently, a long record of around 370 attacks on oil pipelines in Iraq only between 2003 and 2008 by various groups, ISIS' attacks on major oil facilities in Iraq and Syria at least 20 times only between 2013 and 2015, Bangladesh Bank heist of 2016, the WannaTry cyber-attack of 2017 against the UK'S NHS costing around £100 million[xi] are only a quite brief list of many attacks in the past decade against critical infrastructures and it should also be noted that this list does not include one of the categories with highest number of reports and allegations, namely the cyber and physical attacks against Cis directly or indirectly by other states.

Aramco Strikes from The Point View of Critical Infrastructures

With Aramco attacks, the world has seen one of the recent and consequential examples of targeting critical infrastructures. On September, 14 around 04.00 a.m., two of the Saudi Aramco's largest oil facilities were attacked.[xii] Located near the oil-rich province ed-Dammam, Abqaiq and Khurais oil facilities caught fire after being struck by cruise missiles and weaponized drones. Immediately after the attacks, Saudi Arabia did not blame any actor and said that the authorities were working seriously to put out the blaze engulfing the oil facilities.[xiii]

After a little while, the Houthi military spokesman Yahya Sera claimed responsibility for the Saudi Aramco attacks via the Houthi-run al-Masirah satellite channel.[xiv] According to the Houthi militias, the reason for the attacks was to send a signal to Saudi Arabia for its destructive military engagement in Yemen. The Houthi military spokesman proudly announced that "as the Yemeni people" they intend to continue to undertake such attacks in the future as well if Saudi Arabia continues to engage in Yemen militarily.

These attacks have primarily demonstrated one thing. Even Saudi Arabia- whose military spending is one of the highest in the world- has difficulty securing the most valuable resource for its economy and for its survival as well. Therefore, Saudi missile defense systems and its capacity to make them as efficient as possible need to be strengthened in the face of growing threats posed by non-state armed actors in the region.

As a critical infrastructure, the oil-producing sites, oil refineries, and other compounds have been continuously targeted by the Houthi militias for some time. Yet until now, even the Houthi militias could not have carried out such a large attack against the worlds largest oil refineries.

There are two dimensions in analyzing the attacks. One is dwelling on the details on how the attacks came about, who were the culprits and how the attacks were possible. The other dimension is the broader security and foreign policy implications emanating from the attacks.

It is still not crystal clear who was behind the attacks. Also unknown is the place from which the drones aired and the cruise missiles were launched. On the first part, three actors are being evaluated as the possible culprits; the Houthis in Yemen, Iran (by itself or via proxies) and Israel. On the second part, three places come to the forefront; Yemen, Iran, and Iraq. When it comes to the sites from which attacks may have been

carried out, Iraqi officials denied the allegations as did the Iranian officials.

Although the Houthi militias claimed responsibility for the attacks, virtually no one in the western capitals have given credit to this statement. A later statement from the Houthis warning that Iran may be planning an attack against Saudi Arabia confounded the western capitals. The fact that the international media has not given credit to the Houthi statement can be explained by two reasons. One is the continuing doubt about whether the growing military capability of the Houthis could have allowed such attacks to be executed and the other is the idea that the escalating tensions in the Gulf irritated Iran and therefore prompted a response. The third scenario posits that Israel was behind the attacks because of the recent US decisions to ease pressure on Iran by discharging the hawkish National Security Advisor John Bolton and the Trump's backchannel diplomacy with Rouhani through France, Oman and even through the UAE.

After the attacks, the long-time security partnership between the US and Saudi Arabia started to be challenged. Saudi Arabia has built a strong security partnership with the US over the years, being the most loyal customer of the US military technology and equipment. However, the US-made missile and air defense systems -Patriots- could not intercept the drones and missiles, as they were programmed for taking down enemy aircrafts. That incapacity led Saudi Arabia to ratchet up security in the oil facilities and their surroundings. In an effort to assure the Saudis, the Pentagon has announced that 200 troops and Patriot missiles will be sent to Saudi Arabia to

> "The targeting of Abqaiq and Khurais oil facilities is quite important especially because the Abqaiq is the largest oil facility in the world. A former officer in Barack Obama's NSC identified the Abqaiq oil facility as "perhaps the most critical facility in the world for oil supply".

strengthen the defense capabilities of the Kingdom.[xv]

The targeting of Abqaiq and Khurais oil facilities is quite important especially because the Abqaiq is the largest oil facility in the world. A former officer in Barack Obama's NSC identified the Abqaiq oil facility as "perhaps the most critical facility in the world for oil supply". The disruption in the oil production in Abqaiq initially climbed to 5.7 million bpd.[xvi] That disruption prompted a 19 percent spike in global oil prices, shifting the price of Brent crude from 62 USD to 71 USD.[xvii] In accordance with giving assurances to the global oil market, Russia had to stepped in, increasing its daily oil production in the face of Saudi cuts.

The international responses to the attacks on Abqaiq and Khurais oil facilities came immediately after the attacks. Along with Washington, the western capitals Paris, Berlin, and London make a joint statement on the sidelines of the annual opening of the UN General Assembly, accusing Iran of plotting the attacks.[xviii] In response, the Iranian President Hasan Rouhani and Minister of Foreign Affairs, Javad Zarif strongly denied the accusations.[xix] In denying the attacks were plotted by Iran, Zarif said that "any attack ...[on Iran] would lead to all-out war].[xx]

On September, 20, in order to draw Saudi Arabia one step closer to the negotiating table, the Houthi militias announced that they would stop targeting Saudi Arabia and expected it to do the same.[xxi] Hesitated at first, Saudi Arabia later accepted a partial ceasefire in the Houthi-run places. [xxii] The reason why the Saudi Arabia accepted a partial ceasefire might be the idea of creating a division between the Houthi militias or strengthening an existing one. It is widely known that the Houthi militias do not constitute a united front against Saudi Arabia. While some fractions of the Houthi desire for an international recognition as "freedom fighters" or something akin to that while others in the Houthi militias are more radical against Hadi government and its primary supporter Saudi Arabia.

One way or another the ceasefire could be read as an attempt by the Houthis to distance themselves from Iran. Given their statement regarding a possible Iranian attack after Aramco attacks, it may well be reasonable for the Houthis to distance themselves, at least politically if not militarily or logistically, from Iran in the face of US and western pressure.

As for the technical implications of the Aramco attacks, it needs to be acknowledged that the attacks may cause Saudi Arabia to exaggerate the results for strengthening its security cooperation with the U.S. There are rumors saying that Saudi Arabia might be willing for the purchase of s-400 missile defense systems from Russia. This development could be related to the intimate relations of Mohammed bin Salman and Russian President Vladimir Putin and their constant international backing of each other. However, the Trump's immediate "locked and loaded response"[xxiii] and the Pentagon chief Mark Esper's announcement regarding the deployment of troops have demonstrated that a possible shift of axis on the side of Saudi Arabia does not seem likely at this point.

Besides, it is not the first and probably will not be the last time that the U.S. has given security assurances to Saudi Arabia. The Strait of Hormuz and Gulf of Oman have been a theater of war-mongering and chest-humping particularly from May onwards. Following the oil tanker attacks and holding tankers captive, the Gulf has seen a lot of saber-rattling. Together with Aramco attacks, and the continuous insecurities in the Gulf, it could be argued that the American military presence continues to be ratcheted up in the region.

Conclusion

The targeting of Abqaiq and Khurais oil facilities has once again demonstrated that critical infrastructures has become a key target for non-state armed actors whose tactics mostly take a simple but rational calculation into account that with limited resources and relatively quite lower capability, the most critical targets, if possible with an added surprise effect, are the ones that would benefit the groups most and would have the highest impact. Also, the attacks underlined the need to revise and reinforce the defence capabilities in terms of defending CIS since today's war machines as well as the living standards of ordinary people and working political and economic systems heavily depend on the physical and cyber CIs. The asymmetrical threats such as targeting the largest oil refineries in the world with drones and other related equipments signify that if the ways of targeting enemy positions vary, so should the ways of warding it off. In an era of increasing use of drones with various specifics by ISIS, YPG, Boko-Haram, Al-Shabaab and the impressive learning curve of non-state armed actors including terrorist groups regardless of their motivations are taken into consideration, this phenomenon seems to be with us for the future. Since innovation and adaptation become a quite common commodity among such groups also thanks to the increasing use of other innovations, namely social media, messaging apps and streaming outlets, not only more and more critical targets can be more easily selected, but also more and more complicated and effective ways of attacking them with even less costly methods might be the new normal to act against.

However, in the case of the Abqaiq and Khurais oil fields, it has been said that the military technology and the equipment necessary to execute the attacks could not be owned by the Houthis, signalling the close Iranian military support to the Houthis. Although Saudi Arabia conducted an investigation into the attacks and supposedly found Iranian equipment, it is possible that this could be a cover-up or an intentional effort to bring Iran forward. Still, considering the fact that in almost each and every battlefield today, regardless of the scope and severity of the conflict, weaponry and technology can easily be channelled to various other groups on the ground, even such more visible state-non-state cooperation cannot guarantee the limits of the mobility of military hardware.

More important than the details of the attacks is the broader regional and international implications of the attacks. The destructive Saudi military engagement in Yemen and the broader rivalry between Saudi Arabia and Iran are unsurprisingly regarded as the primary causes of the event. Regional rivalries and intensifying proxy wars seem to be the norm rather than the exception for the region both today and possibly in the future. With the increasing tension in the region, higher number of actors getting involved in the conflicts in the region, regime weaknesses and the failure to provide necessary social and economic services, along with the emergence of new non-state armed actors and/or transformation of the already existing ones, the Gulf seems to be more dangerous and insecure than ever in the absence of either reconciliation or the undeniable victory of either side. The Gulf does not need more sabre-rattling, it needs stability, security and peace. Considering the latest news about the Saudi forces' embarrassment in Yemen, however, such a prospect is still quite debatable for the foreseeable future.

Endnotes

[i] The Protection of Critical Infrastructure againstTerrorist Attacks: Compendium of Good Practices, UNOCT, UNCTED, INTERPOL Joint Report, 2018, un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf.

[ii] Resolution 2341, http://unscr.com/en/resolutions/doc/2341

[iii] The Protection of Critical Infrastructure againstTerrorist Attacks: Compendium of Good Practices, p.16.

[iv] Ibid., p. 18.

[v] "Critical Infrastructure Sectors", The U.S. Department of Homeland Security, https://www.dhs.gov/cisa/critical-infrastructure-sectors

[vi] "Critical National Infrastructure", CEntre fort he Protection of NAtional Infrastructure, https://www.cpni.gov.uk/critical-national-infrastructure-0.

[vii] National Security Strategy and Strategic Defence and Security Review 2015, House of Commons, 8 July 2016, https://publications.parliament.uk/pa/jt201617/jtselect/jtnatsec/153/15306.htm

[viii] "Cyber Security of the UK's Critical National Infrastructure", Joint Committee on the National Security Strategy, 2017 , https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf.

[ix] "Critical Infrastructure", European Commission, https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf and Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

[x] Gerry Oberst, "Protecting Satellites From Space Terrorism", ViaSatellite, 1/3/2009, https://www.satellitetoday.com/uncategorized/2009/03/01/protecting-satellites-from-space-terrorism/; Tom Ball, "Top 5 critical infrastructure cyber attacks", Computer Business Review, 18/7/2017 and Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say", The New York Times, 6/7/2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

[xi] Iraq Pipeline Watch, Institute for the Analysis of Global Security,27/3/2008, http://www.iags.org/iraqpipelinewatch.htm; "PKK İdil'de Kerkük-Ceylan boru hattına saldırı düzenledi", Haber Türk, 27/2/2016, https://www.haberturk.com/gundem/haber/1201949-pkk-idilde-kerkuk-ceyhan-boru-hattina-saldiri-duzenledi; "PKK'dan boru hattına bombalı saldırı", CNN Türk, 26/10/2012, https://www.cnnturk.com/2012/turkiye/10/26/pkkdan.boru.hattina.bombali.saldiri/682093.0/index.html; "Kerkük-Yumurtalık hattına sabotaj", CNN Türk, 19/1/2013; "Kerkük-Yumurtalık boru hattında patlama", CNN Türk, 22/4/2010, "Petrol boru hattına sabotaj, CNN Türk, 6/5/2009; "Boru hattındaki yangın PKK sabotajı

"CNN Türk, 24/11/2008;"Rocket Strikes Site of Major Oil Companies in Iraq's Basra amid Heightened US-Iran Tensions", SouthFront, 19/6/2019, https://southfront.org/rocket-strikes-site-of-major-oil-companies-in-iraqs-basra-amid-heightened-us-iran-tensions/; Tracy Kitten, "Bangladesh Bank Heist: Lessons Learned", Bank Info Security, https://www.bankinfosecurity.com/bangladesh-bank-heist-lessons-learned-a-9064; "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled", The Telegraph, 11/10/2018, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[xii] Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran (Accessed: 14/09/2019) https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

[xiii] Explosion and fire reported at Aramco site in Saudi Arabia (Accessed: 14/09/2019) https://www.alaraby.co.uk/english/news/2019/9/14/explosion-reported-at-aramco-site-in-saudi-arabia

[xiv] Major Saudi Arabia oil facilities hit by Houthi drone strikes (Accessed: 14/09/2019) https://www.theguardian.com/world/2019/sep/14/major-saudi-arabia-oil-facilities-hit-by-drone-strikes

[xv] New U.S. Aid to Saudi Arabia Will Include 200 Troops (Accessed: 26/09/2019) https://www.nytimes.com/2019/09/26/world/middleeast/troops-defense-saudi-pentagon.html

[xvi] Saudi Aramco reveals attack damage at oil production plants (Accessed: 20/09/2019) https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html

[xvii] Oil prices soar after attacks on Saudi facilities (Accessed: 17/09/2019) https://www.bbc.com/news/business-49710820

[xviii] France, Germany, and UK say Iran is responsible for attacks on Saudi Arabia (Accessed: 23/09/2019) https://www.vox.com/world/2019/9/23/20880639/france-germany-uk-iran-saudi-statement

[xix] Iran rejects fresh accusations over Saudi oil attack (Accessed: 24/09/2019) https://www.bbc.com/news/world-middle-east-49805591

[xx] Military strike against Iran would result in 'all-out war':Zarif (Accessed: 19/09/2019) https://www.reuters.com/article/us-saudi-aramco-zarif-war/military-strike-against-iran-would-result-in-all-out-war-zarif-idUSKBN1W41II

[xxi] Yemen's Houthis say will stop all attacks on Saudi Arabia (Accessed: 20/09/2019) https://www.aljazeera.com/news/2019/09/houthis-stop-attacks-saudi-arabia-190920183802126.html

[xxii] Saudi Arabia agrees to partial ceasefire in Yemen (Accessed 27/09/2019) https://www.middleeasteye.net/news/saudi-arabia-agrees-partial-ceasefire-yemen-report

[xxiii] Trump: US "locked and loaded depending on verification" of attack on Saudi oild fied (Accessed: 16/09/2019) https://edition.cnn.com/2019/09/15/politics/trump-us-saudi-arabia-attack-iran-iraq/index.html

Notes

ORTADOĞU ETÜTLERİ

MIDDLE EASTERN STUDIES

Hakemli Siyaset ve Uluslararası İlişkiler Dergisi

ORSAM Publishes

Middle East Analysis and Middle Eastern Studies as periodical journals. Middle East Analysis, which is published bimonthly in Turkish, covers the expert opinions on contemporary developments in the Middle East. Middle Eastern Studies is a semi-annual journal on international relations. As a scholarly and refereed journal, published in both Turkish and English, Middle Eastern Studies is composed of the contributions of academics who are experts in their field. Middle Eastern Studies, where respectable, national and international level academics publishes their papers, is indexed by Applied Social Sciences and Abstracts (ASSIA), EBSCO Host, Index Islamicus, International Bibliography of Social Sciences (IBBS), Worldwide Political Science Abstracts (WPSA).

Ortadoğu Araştırmaları Merkezi
ORSAM
مركز دراسات الشرق الأوسط

Mustafa Kemal Mah. 2128. Sok.
No:3 Çankaya/Ankara

+90 (312) 430 26 09
+90 (312) 430 39 48

info@orsam.org.tr
www.orsam.org.tr

orsamtr