



LUDOVIKA
UNIVERSITY PRESS

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY
AND PUBLIC MANAGEMENT SCIENCE

Volume 19 (2020)
Issue 3

ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security and public management.

AARMS is published in one volume of three issues per year by the University of Public Service, Budapest, Hungary, under the auspices of the Rector of the University.

Articles and other text material published in the journal represent the opinion of the authors and do not necessarily reflect the opinion of the Editors, the Editorial Board, or the Publisher.

All correspondence should be addressed to Prof. PADÁNYI József, PhD, Editor-in-Chief,
University of Public Service
P. O. Box 15, H-1581 Budapest 146 Hungary
aarms@uni-nke.hu

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY
AND PUBLIC MANAGEMENT SCIENCE

Volume 19
Issue 3
2020

An International Journal of Security, Strategy, Defence Studies,
Military Technology and Public Management
Published by the University of Public Service
PADÁNYI József (Chair of the Editorial Board)
SOLYMOSI József (Honorary Chair of the Editorial Board)

Editorial Board:

BLAHÓ András	Pavel MANAS
Vasile CĂRUȚAȘU	NÓGRÁDI György
Erich CSITKOVITS	ONDRÉK József
Boris DURKECH	Boguslaw PACEK
HAIG Zsolt	Harald PÖCHER
HALÁSZ Iván	SZENES Zoltán
KENDE György	TAKÁCS Péter
Ulrike LECHNER	TAMÁS András
TÖRÖK Gábor	

Editorial:

PADÁNYI József (Managing Editor)
GAZDAG Ferenc (Editor)
HALÁSZ László (Editor)
ORBÓK Ákos (Editorial Assistant)

Publisher:

University of Public Service, Ludovika University Publishing House
Responsible for Publishing:
KOLTAY András, Rector

Copy editor:

GERGELY Zsuzsánna

Typeset and print by Pátria Printing House Co.
ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

Contents

Ferenc KOCZKA:	
Security of Encryption Procedures and Practical Implications of Building a Quantum Computer.....	5
József PADÁNYI – József ONDRÉK:	
The Impact of the Covid Pandemic on Security and the Military: Civil-Military Cooperation in the Fight against the Covid Pandemic.....	23
György GULYÁS – Árpád POHL:	
The Role of the NATO Support and Procurement Agency in Support to Operations.....	37
Tibor BABOS – Gábor SINKÓ:	
Can Boko Haram Constitute a Threat to European Security?	53
Péter SELJÁN:	
Military Intervention and Changing Balance of Power in Libya	71
Gábor SELJÁN:	
The Remarkable 10 th Anniversary of Stuxnet.....	85

Security of Encryption Procedures and Practical Implications of Building a Quantum Computer

Ferenc KOCZKA¹ 

In ensuring the operation of an IT system, it is essential to maintain the data's confidentiality and integrity, which is based on some encryption processes. Encryption procedures are based on algorithms, the theory of which is given by cryptography. Due to their complexity, they are often hardly understandable not only to an average person but also to the majority of professionals who are familiar with IT. The algorithms used are not eternal; various designs or implementation errors or even performance gains from computer hardware improvements make one time high achieving algorithms obsolete and easily hackable. Strong algorithms can be circumvented in alternative ways, the necessary software and hardware infrastructure can already be built from personal computing devices. I tested its effectiveness on two different password databases: with the success of hacking university passwords, I prove that it is possible to circumvent strong algorithms with simple methods. Modern encryption algorithms have a relatively long life cycle and they become obsolete slowly. The construction of the quantum computer creates a new situation, which requires a number of procedures to be eliminated and its parameters to be modified or protected by additional methods. As it is an impossible task to modernise the encryption algorithms of all IT systems operating today, preparations must be started as soon as possible so that the new situation can be handled, at least for critical systems. In my article, I would like to draw attention to the weaknesses of encryption methods, present a possible method of circumventing the cryptographic methods currently in use, demonstrate the operation of a quantum computer and some algorithms relevant to the topic.

Keywords: encryption, hash code, password security, crack, quantum computer

Introduction

Most IT tools include some kind of encryption process, which is largely responsible for confidentiality and integrity, especially for the implementation of secure communication and data storage. Their application is unavoidable as there is no guaranteed technical

¹ Director of IT, Eszterházy Károly University; e-mail: koczka.ferenc@uni-eszterhazy.hu

possibility of preventing network communications interception, so those requirements can only be ensured by using encryption procedures. The theoretical support for hiding data is the task of cryptography, which has developed several procedures to achieve this goal. The use of cryptography in modern warfare is also essential. The usual practice of military developments being transferred to the civilian sphere has now been reversed after a while, so many military solutions build on public procedures to meet specific requirements.

These algorithms also play a role in counter-terrorism protection. Eavesdropping on terrorists' communications, preventing the communication capabilities of attack equipment built almost exclusively from ordinary devices, is impossible without cryptography. Several everyday devices can be used to activate a bomb: a mobile phone, garage opener, CB radio, wireless bell, or even children's toys. The Ukrainian Aerorozvidka group used a self-built drone to carry out successful military reconnaissance and data collection tasks.² The difficulty of this task is the use of a set of tools using various forms of communication. However, the IT procedures used in battlefield communication are different from those used in civilian life. The main reason for this is low computing power for low energy consumption and limited data transfer speeds available in combat conditions, which in many cases is only a fraction of what is common in everyday life.

An important goal of electronic protection is to intercept the enemy's communications, which is an important element in developing information superiority. Nowadays, warfare is present not only on the battlefield but also in civilian life, the protection of communications between constituents of national security importance turned to an essential task. Although not recognised by most states, detecting and purchasing security holes of computer systems³ are generally used for developing offensive cyber weapons.⁴

Therefore, cybersecurity success depends greatly on the functioning of the cryptographic algorithms used; their vulnerability and inadequate implementation can have serious consequences.

Historical overview

From the point of view of warfare, important encryption procedures date back to ancient times. One of the first procedures is called the Caesar method, whose algorithm is very simple. It mingles each letter of the alphabet with another one at a certain distance to quickly encode the text to be encrypted and decode it at the destination. Although the procedure was considered safe at that time (even literacy was not typical), today, messages encrypted using these types of methods can be decoded in no time. Trying out possible cases is only one option because if the message's language is known, the frequency of characters in the message can also be an easy guide to determine which character has been replaced by which one. However, throughout history, especially in warfare, some variant of Caesar's method

² Péter Huszár, 'Ukrajna közösségi finanszírozású, katonai célokat szolgáló oktokovertéinek elemzése', *Hadmérnök* 14, no 2 (2019), 34–43.

³ The Zerodium offers a high amount for vulnerabilities not published elsewhere. See <https://zerodium.com>.

⁴ PA Media, 'UK has mounted covert attacks against Russian leadership, says ex-mandarin', *The Guardian*, 24 October 2020.

has been used on many occasions. The timeliness of the solutions based on the exchange of letters remains current in many modified versions, even in the two world wars.

In the history of encryption, we find some methods and tools, one of the most well-known of these was the German-made Enigma, which appeared in World War I and was used until the 1970s to encrypt and decrypt radio messages, which, through continuous developments, included a family of machines operating along with an increasingly complex set of rules. There was only a small chance of breaking the encryption of Enigma machines at the era's technical level. Combinations of rotors provided encryption, and the high number of variations made it impossible to decrypt the encrypted message in real-time. The practical procedure used by Enigma had several weaknesses. Due to the use on the battlefield, the risk of key transmission must be taken into account. Its cryptographic weakness stems from the very large keyspace defined by the equipment. The encryption was determined by the set of used rotors, their order and positions. In total, they gave 2,109,120 different options, which were not impossible to decrypt even in World War II by the try-and-try method.⁵ As a result, one of the greatest minds in IT, Alan Turing, built a machine that could eventually be successfully used to decrypt battlefield messages, making it a major part of the war's outcome.

The development of encryption procedures and the competition for research into their hacking have accelerated with the appearance of electronic computers, and relatively demanding procedures can be quickly operated. Along the lines of modern mathematical approaches, many methods have been found that seem hopeless to crack today.

Encryption methods

There are several types of encryption procedures, but there are three types to address for our topic. In most cases, symmetric encoding is used to transmit encrypted messages after a key exchange using public-key encryption, and hash algorithms are used to verify (but not only for that purpose) integrity.

When symmetric key encryption is used, the key used for encrypting and decrypting is the same and can be used to encode and decode a message. Several great algorithms such as this are known as typical examples of highly complex 3DES or AES. These use the key in mathematical formulas to create an encrypted form of the message through multiple substitutions. Without knowing the key, decryption is not real with today's IT tools. The great advantage of symmetric encryption procedures is speed; the performance of most algorithms is sufficient to encrypt large amounts of data in a short period. In the case of Enigma, the key is the type of rotors used to encode the message, their initial positions, and the staple board settings. The key transmission plays an extremely important role in the process and in World War II, it caused a fatal error in the defence of the Navy's M3 model.

⁵ Richard E Klima and Neil P Sigmon, *Cryptology: Classical and Modern* (Chapman and Hall/CRC Press, 2018).

The machine acquired during the interception of the U-110 submarine, and the documents requiring its settings allowed the Navy's messages to be decrypted for nearly 9 months.⁶

Public key encryption works completely differently from the point of view of the key. It is based on a pair of keys generated using an open process, using large prime numbers. One element of the key pair is made the public key, and the other is treated as the private key and is prevented from being known to others. The key pair is special in that a message encrypted with one party can only be decoded with the other party (that is, not with the encoding party itself). A public key encryption data is always performed with the public key of the target person or device, taking advantage of the knowledge of the private key that it owns to decrypt it. This procedure also implements the digital signature by encrypting the message with the sender's private key, the authenticity of which can be verified by decoding with the sender's public key.

These algorithms are not affected by the problem of key transfer. Therefore, they can ensure confidentiality and integrity, even in cases where the sender and receiver's entire communication is intercepted. Their practical usage, on the other hand, is greatly hampered by their high computing expectation. Perhaps the most popular members of this family are RSA and DSA. The combination of the two methods can eliminate their disadvantages. In many cases, including SSH operation,⁷ public key encryption is used to create a secure connection, but this is only used until the symmetric key is transmitted. After a successful key exchange, the connection is continued with fast-functioning symmetric key encryption.⁸

In addition to encryption procedures, the priority area for our topic is the so-called hash algorithms. These algorithms do not actually encrypt, they just create a short code, named hash, from a series of data of any length.⁹ Therefore, the hash is not the encrypted form of the original data series, from which the original series cannot be restored; it only allows to check its integrity. To do this, you need to re-calculate the hash value for the series and compare it to the original. Since changing the source involves a radical change in the hash, any modification is very easy to detect. Well-known hash procedures are variants of SHA¹⁰ of varying strengths.

From a cryptographic point of view, hash algorithms also play a major role, from checking the integrity of transmitted data to the operation of several cryptocurrencies in network communication. Hashing procedures are also widely used when storing passwords. In most systems, to prevent an attacker from knowing the cleartext passwords in a system when user data is compromised, only the hash values that are made from them are stored, not

⁶ Forces.net, 'The First Man To Storm A Nazi U-Boat And Seize An Enigma Machine', 06 January 2016.

⁷ SSH stands for Secure Shell, which is the name of a computer protocol and the program that uses it. Using strong encryption, it implements a number of functions: it allows you to log on to remote computers, copy files and create encrypted tunnels.

⁸ Daniel J Barrett, Richard E Silverman and Robert G Barnes, *SSH, The Secure Shell: The Definitive Guide* (Sebastopol: O'Reilly, 2001).

⁹ Donald E Knuth, *The Art of Computer Programming* (Boston: Addison-Wesley, 1973).

¹⁰ The first version of SHA was published in 1993 and was provided in several versions (SHA-224, SHA-256, SHA-384 and SHA-512). The mining of Bitcoin actually means training mass SHA-256 hashes and finding an instance with a specific property.

the password itself. When a user logs on, the hash from the specified password must match the one stored in the system to allow access.¹¹

Cryptographic algorithm errors

During the development of computing devices, many algorithms that had previously been widely used proved weak. The vulnerable md5 algorithm is already discouraged; therefore, all devices had to be replaced which contained it. This procedure is simple in systems where the developer still supports the software and knows its users so that the upgrade can be carried out, and the modified component can be sent to the destination. On the other hand, hardware and software components no longer supported or whose operators cannot be notified to perform the upgrade are more difficult tasks. Equipment designed to keep production costs low to such an extent that the device cannot run a component with higher computing needs at an acceptable speed is a separate category, typical examples of which are IoT devices.¹²

In principle, the exchange of procedures may be necessary for two reasons: a conceptual error in the algorithms used or an implementation error. The latter is caused in most cases by some programming error that weakens the otherwise well-functioning algorithm. Typical sources were faulty random number generators, which did not generate random numbers, so instead of unpredictable input data guaranteeing correct operation, they provided reproducible or repetitive input. Such an implementation error can be caused by leaving key data in memory after the code runs or making it available to other applications. In the case of Enigma, the implementation error is the constraint on the type of rotors selected, their order and their initial settings, which drastically reduced the size of the keyspace as described above. Implementation errors are characterised by the failure of only one operating system or device, while they do not occur in the case of other users of the same procedure.

Conceptual errors in algorithms are much more serious problems. An example that still affects many systems today is KRACK (Key Reinstallation Attack). This vulnerability affected the WPA2 algorithm; therefore, almost all Wi-Fi devices became unsafe,¹³ and providing updates took months.¹⁴ As the error was in the algorithm itself, many devices became vulnerable at the same time, regardless of their operating system. In the case of KRACK, the situation is further exacerbated by never updating the operating system of

¹¹ Because the same hash value can come from several different input data, this method may allow access with a different password.

¹² Internet of Things (IOT) devices are low-performance IT devices that are typically able to collect and transmit information over the Internet at low power consumption.

¹³ The whole point of vulnerability is when a wireless network connection is established, the client (computer, mobile phone, and so on) initiates a connection request to the network device (for example, Wi-Fi router). The connection is technically the result of a multi-step dialog, in the third step of which the two parties are identical to the encryption key used. Because a network error can occur at any time during connection creation, such as during this step, the procedure is able to resend this encryption key. An attacker could use this to collect and re-send these keys, forcing the device to reset its own internal counter (nonce). Because the algorithm is only secure if this counter is not repeated, this procedure can be used to break it.

¹⁴ Mathy Vanhoef and Frank Piessens, 'Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2', *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, October 2017, 1313–1328.

some of the users' wireless network devices, which does not appear on old systems so that the error will be exploitable for years.

Brute force methods

One of the recipes for breaking an encrypted communication is to reduce the keyspace as much as possible and then try through possible combinations in as short a time as possible. The reduction can usually be made with higher mathematical knowledge, but the amount of time it takes to try depends mostly on the computing power of the computer used.

With the release of cryptocurrencies, many specialised devices with previously unimaginable computational power appeared on the market using this technique. Their purpose is mass hash computing, which was used to mine cryptocurrencies. The Antminer S19 Pro¹⁵ is capable of 110 Terrahash per second with 3500W power consumption. Higher-value VGA cards can also be used to solve such tasks. Their processors (GPU – Graphical Processing Unit) are significantly faster than the processors of commonly used computers, so they are also suitable for brute force methods.

One of the most important motivations for cyberattacks is to obtain personal and economic data and access parameters. One way to protect them is encrypted storage, in particular access passwords, recorded in a readable form instead of the hash mentioned above value, which is now a professional error. Although the GDPR does not impose specific requirements on passwords, it does provide for sanctions in the event that an organisation leaks large amounts of personal information. That is the reason why it is not in the organisations' interest to store readable passwords. No legislation formulates any specific encryption procedure, so it is up to the developer to choose and implement its method.

The need to encrypt passwords in this form is also demonstrated by the fact that the systems of the world's largest IT companies have also been hit by cyberattacks in which large-scale personal data has occasionally been compromised by passwords, but mostly only by hashing it and has been offered for sale to spamming service providers, or on the Darknet.¹⁶

Check password hash cracking using traditional tools and methods

IT professionals are also divided on the chances of breaking different encryption procedures or hashing out original passwords. Internet sources provide measurement results on the speed at which systems developed along a specific hardware and software environment can generate password hash values.¹⁷ These often refer to raw data and do not take into account

¹⁵ For more details see <https://miners.eu/product/bitmain-antminer-s19-pro-110th-bitcoin-miner>

¹⁶ On *haveibeenpwned.com* page, you can examine whether a specific email address was involved in an incident that is currently being investigated. Their database contains more than 10.5 billion records. The site also provides information about data breaches, which include very popular, large companies such as Adobe and Dropbox.

¹⁷ The results of the series of measurements using the NVidia GTX-1080 VGA card with Hashcat software on a Linux operating system. See <https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40>

users' password-training habits and fine-tuning techniques for brute force. To test this, I took measurements on the directory containing the real password impressions of Károly Eszterházy University (EKE).

Since the university's central IT organisation provides complex services with many different systems, several different hash values of passwords have been recorded in the central directory. This provided the opportunity to examine the strength of NTLM and SHA-1 hash algorithms.

An I5-based Linux desktop computer carried out the test with an SSD, in which an NVidia GTX Titan VGA card provided the necessary computing capacity. Hash computing was done with HashCat¹⁸ software, which can use the GPU of the VGA card to perform the task. The time required for each measurement was capped at four days.

HashCat is not only capable of searching for a password for a hash but can also batch-operate by trying to crack all elements of a file containing hashes in a single operation. To be able to tune the hacking process, HashCat allows you to set so-called masks. These are regular expressions that can define specific password forms by describing the characters that can stand in each position. The suitable settings for masks greatly affect the effectiveness of decrypting passwords; in our experience, special characters are typically used by users towards the end of the password.

In the first phase of the test, I examined the 2650 NTLM password hash values by tuning the software's operation with different masks. We conducted the test in five different configurations:

1. No fine-tuning was performed in the default setting (default mask) test.
2. We did not refine the search process in the full ASCII namespace setting, that is, we attempted to find all possible passwords.
3. We tested different variants when applying our masks; the best result was given by the third. We assumed that either position could consist of upper- and lower-case letters, digits, and special characters for passwords of six characters or less. For longer ones, a special character was assumed in only two positions, and in the others, only lowercase or number.

Table 1 shows the number of compromised passwords based on their length.

Table 1: NTLM password length and the number of cracks

Hits	Password length					
	4	5	6	7	8	9
Default mask	2	11	26	25	186	117
Full ASCII namespace	2	11	28	26	–	–
Own mask 1	2	10	27	24	25	13
Own mask 2	2	11	28	25	435	–
Own mask 3	2	11	28	25	435	154

Source: Compiled by the author.

¹⁸ For more information see <https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40>

The measurement shows that it was not practical to examine the entire namespace when cracking NTLM passwords. It performed better when examining 7-character passwords, but for 8- and 9-character passwords, we had to give up because of a very high run time. The best result was achieved with the type 3 mask, which decrypted a total of 655 passwords, which is 24.7 per cent of the total password space.

The time required for the above results is given in Table 2. According to this, the time needed to crack passwords was less than one second for six characters, and decrypting the eight-character passwords did not require too many resources. Therefore, based on the time data, 9-character passwords cannot yet be called secure, so it can be concluded that longer passwords must be required to be secured.

Table 2: NTLM password cracking times

Running times	Password length						
	4	5	6	7	8	9	
Default mask	~0s	~0s	~0s	23s	18m 35s	12h 41m	
Full ASCII namespace	~0s	3s	2m 14s	3h 39s	Not measured	Not measured	
Own mask 1	~0s	2s	5s	2m 34s	1h 54m	3d 5h	
Own mask 2	~0s	~0s	19s	5m 40s	4h 8m	Not measured	
Own mask 3	~0s	1s	19s	3m 13s	2h 18m	3d 21h	

Source: Compiled by the author.

Breaking the 2194 SHA1 hashes has proved to be a more difficult task. Due to the complexity of the procedure, the GPU of the VGA card produced fewer hashes in a time unit. The time available to decrypt the nine-character passwords was not enough, but compared to the previous values of NTLM cracking, it can be concluded that the result is not far behind in terms of success. However, the time taken to calculate was about tripled. Overall, 470 passwords were broken, which means a result of 21.4 per cent.

Table 3: SHA-1 password length and the number of cracks

	Password length				
	4	5	6	7	8
Number of variations	2,40x10 ⁷	1,68x10 ⁹	1,18x10 ¹¹	1,02x10 ¹²	4,18x10 ¹³
Running time	~0s	~2s	1m 6s	10m 55s	7h 24m
Hits	2	11	21	22	414

Source: Compiled by the author.

Overall, it can be concluded that with a computer worth approximately HUF 200,000, the optimal setting of the hacking software, more than one-fifth of the organisation’s passwords could be decoded in less than four days. By measuring, I found that 8-character passwords no longer provide sufficient protection.

Data on the Darknet

When examining password security, one must ask the following question: How many institutional email addresses were found in databases that have been stolen from companies that manage them? These addresses appear not only in the address lists that are the source of spam but also in databases with other data, obfuscated or readable passwords, for example, on the Darknet. To look at the extent to which email addresses of Eszterházy Károly University have been affected by these attacks, I have used a collection of more than ten billion records available at <http://haveibeenpwned.com>. The site's database of 485 different data breaches at the time of writing these lines contains 10.5 billion data access. Anyone can check which incident or collection their email address¹⁹ was involved in. Bulk verification can be done²⁰ through so-called API calls, which I used in the verification software.

When examining email addresses, I used the university's full address list, which included not only the live addresses but also the delisted addresses, including the institution's previous domain,²¹ which justifies the number of email addresses high relative to the size of the institution. The measurement results showed a very favourable condition; only 50 out of the 6,386 email addresses were found in this database, which is less than 1 per cent. These email addresses have been involved in 11 different incidents, a total of 87 times, so overall, it can be established that the email addresses of the University of Eger were only minimally present in these databases. The details are summarised in Table 4.

Table 4: Data leaks and the number of email addresses affected

#	Source	Number of hits
1.	Collection #1 [Collection1] 2019-01-07	52
2.	2,844 Separate Data Breaches [2844Breaches] 2018-02-19	11
3.	Canva [Canva] 2019-05-24	6
4.	Covve [db8151dd] 2020-02-20	5
5.	Apollo [Apollo] 2018-07-23	4
6.	Onliner Spambot [OnlinerSpambot] 2017-08-28	2
7.	Exploit.In [ExploitIn] 2016-10-13	2
8.	Anti Public Combo List [AntiPublic] 2016-12-16	2
9.	LinkedIn [LinkedIn] 2012-05-05	1
10.	Edmodo [Edmodo] 2017-05-11	1
11.	Data Enrichment Exposure From PDL Customer [PDL] 2019-10-16	1

Source: Compiled by the author.

¹⁹ In addition to data obtained during multiple specific attacks, the site database contains data from other partially known incidents. The attackers sold them as collections named by them or the site operator.

²⁰ The Application Programming Interface (API) is a way of communication developed between programs. For haveibeenpwned.com, this is currently available as a monthly service.

²¹ Prior to its change into a university, EKE operated its correspondence under the *ektf.hu* domain, which was replaced to *uni-eszterhazy.hu* in 2015. These types of changes are expected to occur in large numbers as a result of the ongoing reorganisation of universities.

The leakage of these 10.5 billion records does not mean that it contains passwords in readable format. These are often coded, so they are not usable but leaked in coded form. Examination of the university password database, on the other hand, points out that the theoretical security offered by the algorithms does not necessarily work well in practice. To improve the efficiency of encryption, industry-leading companies apply a number of security modifications to their software. Google has made it impossible for Chrome users to download files from pages that use https unencrypted (http).²² Apple has reduced the validity of Safari browser certificates from two years to one, shortening the useful life of any compromised keys.²³ Safari also regularly checks the passwords stored in the user profile and alerts you if any of them have previously been made public.

Our investigation of password cracking was effective up to nine-character passwords. With more investment, this can be increased by additional characters, but the required computational capacity is multiplied by each character. This is why in many cases it is not worth experimenting with brute force methods, so hackers prefer to use phishing or social engineering methods. In a 2018 measurement, also at EKE, using social engineering methods, 17.3 per cent of users' passwords were obtained. Based on my measurement, it can be concluded that the efficiency of SE, which is much easier to implement, does not differ significantly from the 24.7 per cent and 21.4 per cent results measured in the present research.

Administrative regulations

Public communication services based on algorithms providing strong encryption are also a problem for defence organisations in nations. Well-known encryption procedures that are truly unbreakable or unrecognisable due to the transmission of an encrypted message put state law enforcement at a serious disadvantage.²⁴ Because some encryption procedures cannot be avoided from a technical point of view, administrative methods can solve the problem. The relationship between the largest IT companies and the authorities does not go beyond professional rumours. Still, in addition to the United States of America, the idea of restricting or weakening encryption algorithms and prohibiting applications using end-to-end encryption has already been raised in the Hungarian Government. In 2017, the Hungarian Government drafted a proposal that would have prohibited the use of communication applications. The authorities can exercise its right of access, but this was not finally accepted.²⁵

However, the interception and processing of digital signals (SIGINT) are not illegal in all countries. A prominent example is the Echelon network, which aims to support SIGINT

²² For more details see <https://blog.chromium.org/2020/02/protecting-users-from-insecure.html>

²³ See www.thesslstore.com/blog/ssl-certificate-validity-will-be-limited-to-one-year-by-apples-safari-browser

²⁴ For example, steganography is the science of hiding a message in a normal message. In most cases, the message itself is hidden in an image or audio file during practical implementation. Many free programs are available to achieve this service.

²⁵ Bitport, 'A titkosítás tiltása veszélyes', 30 March 2016.

operations, intercept and decipher private and business encrypted communications.²⁶ Its members were the states that accepted the UKUSA agreement, originally established by the NSA (National Security Agency) and GCHQ (Government Communications Headquarters). The International Surveillance Alliance, known as the Five Eyes, which is made up of the United Kingdom, USA, Canada, Australia and New Zealand, is the main objective of electronic intelligence.²⁷

As a result of government-level support for these organisations, so-called backdoors are installed in the source code of some applications, ensuring that the authority can decrypt encrypted communications, review the service provider's event logs, and reveal the identity of the participants in the communication. General providers offering confidentiality of communication (typically VPN providers) are of great importance, and it is appropriate to establish, promote and control them with state aid. However, these methods do not work for software that implements encryption on endpoints, for example, the parties' devices involved in the communication. Besides, open source code can be a safeguard for the program's integrity.

Backdoors are considered dangerous by most IT security professionals, both in encryption algorithms and in applications. Keeping them secret is almost impossible, promotes crime in the wrong hands, undermines trust in IT systems, and would have a seriously debilitating economic effect. Therefore, the social acceptance of these methods is low. Their operation encourages civil society to transfer its network connections through less supervised zones, with which it is likely to have the opposite effect.

The quantum computer

Although most of the algorithms used today with traditional computing tools provide adequate protection with careful use, new technology is imminent that will completely revolutionise the IT world based on current cryptography; this is the quantum computer. Therefore, it can be assumed that preventing the leakage of data protected by encryption today will be even more important.

How a quantum computer works

The operation and algorithms of a quantum computer are significantly different from those of a traditional computer. The basic operating unit of a classic electronic computer is a two-stage unit. A bit can be used to store both the instructions of the program code and its associated data. A bit can take exactly one value at a time, either 0 or 1, which can be read at any frequency during operation.

²⁶ Franco Piodi and Iolanda Mombelli, *The ECHELON Affair* (Luxembourg: European Parliament, 2014).

²⁷ Organisations known as the Nine Eyes and Fourteen Eyes were created with the expansion of the Five Eyes, with the same purpose.

The structure of the quantum computer is different, based on some quantum physics phenomenon, so that the behaviour of suitable particles controls its functioning. Its base unit is the quantum bit, or qubit, which has completely different properties from classic bits, not only in the states 0 and 1 but also in between, at which point the qubit is in a superposition. Intermediate forms can describe many options, so a qubit can store many traditional bits of information that rise by the number of qubits on the machine: n quantum bits correspond to 2^n classic bits. According to this analogy, 300 quantum bits could handle more numbers than the amount of atoms existing in the universe.²⁸

Several methods are known for the physical implementation of the qubit. In addition to the spin of an electron or nucleus, the polarisation of light, the number of electrons or photons, other quantum physics phenomena can also be used. Understanding the machine's physical structure without quantum mechanical knowledge is hardly possible; it is necessary to imagine a basic physical environment unknown in the macroworld. An elemental particle can be present at the same time at two different points in space. It is also a consequence of the physical nature of quantum phenomena that the computed results are only probabilities in themselves and reading the state of the qubits describing the result means an irreversible change in the state.

The inner workings of a quantum machine are also unusual for a traditional programmer. Even basic operations such as value assignment or initialisation are not trivial, and the content of a variable is lost when the calculated value is read out. This is the operational feature that requires programming of the quantum machine along completely new methods, adding that the execution of its program is not linear, generating all the results in one step. The result calculated by the quantum machine is not always correct, so it is natural to have a sometimes incorrect calculation result – one of the goals of the developments is precisely to reduce the likelihood of errors.

The quantum machine is currently highly sensitive to environmental impacts, so several problems still need to be solved to be universally usable. Due to environmental disturbances, it can be operated around absolute zero degrees, although there are also references to a solution functioning at room temperature.

Based on the above, it can be seen that usable quantum computing is currently in its infancy. IBM, MIT, the University of California and Oxford University built a rudimentary machine as early as 1998, with a processor of hydrogen and chlorine atoms. This was only suitable for a few basic operations as they could not run more serious algorithms on it. In addition to Google, Intel and IBM, Alibaba has already built such machines. Since the number of qubits greatly determines the machine's performance, the power rule doubles each additional qubit, so Google's 72 qubits machine can already carry an enormous capacity. Some sources say it will take much more than that,²⁹ with the number of qubits needed to hack 2048-bit RSA at 4,096.

Even if quantum machines are only partially used due to their extremely high prices, they will double impact IT systems. Still, the use of these machines is unlikely to replace

²⁸ Charles Q Choi, 'IEEE Spectrum', *IEEE Spectrum*, 21 May 2020.

²⁹ Aleksey K Fedorov, Evgeniy O Kiktenko and Alexander I Lvovsky, 'Quantum computers put blockchain security at risk', *Nature* 563, no 22 (2018), 465–467.

traditional computers. They should be used in areas that require high computational capacity and can be described with quantum algorithms. No concrete results are currently known, and the expectations are highlighting cryptography in addition to material design, weather modelling and other demanding tasks. The possible use of the quantum computer is mentioned in four key topics in scientific articles. In terms of our topic, the two most important are quantum computing and algorithms and quantum internet. Quantum sensing and metrology is mostly focused on improving the operation of a quantum computer, and quantum simulations are focused on researching high-complexity simulations with a quantum computer.

Quantum computing and Q-algorithms

Quantum computing is perhaps the most researched field. However, in the latter area, there are already results that make it clear that the quantum machine is changing the applicability of traditional cryptographic methods, implementing new foundations for encryption of communication and digital signatures. Therefore, in critical areas, standard encryption procedures need to be reconsidered; otherwise, encrypted information will be hacked by the quantum machine in the foreseeable future. For protection purposes, each affected node's direct connection can be a solution, preventing access to encrypted information by third parties.

However, the most important step is to implement new encryption features or quantum-proof existing ones to be produced on traditional machines and prevent quantum dominance for the future. A vast amount of research is aimed at creating Q-algorithms and mathematically proving their functionality. The practical use of this area is essential not only in cyberspace operations and cyber warfare, but also in the communication of economic and political actors and systems.

The algorithms written on the quantum machine were ahead of their time due to construction difficulties and could not be tested. However, because of the expected environment, those that could be operated immediately when a working machine was available could be developed.³⁰ The Lov Grover algorithm guarantees a result in an unsettled database under the square root of the number of items instead of the serial search method. From a defensive point of view, one of the most important algorithms is the Shor algorithm, which can also be used to crack a very widely used algorithm of public key encryption, RSA.

The Shor algorithm designed for a quantum machine specifies the prime-factor resolution of an integer that plays a role in several encryption algorithms,³¹ which is why

³⁰ For experimental purposes, D-Wave Systems has developed a 2,000 and then 4,000-qubit quantum machine simulator that is suitable for testing algorithms but cannot actually achieve results.

³¹ Peter W Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *Society for Industrial and Applied Mathematics* 26, no 5 (1997), 1484–1509.

it focuses on numerical research.³² Although the problem does not seem particularly difficult at first sight, this is a serious algorithmic difficulty in case of large numbers. RSA Laboratories investigates the number of numbers for which prime resolution can be found, thus breaking encryption, which was the last time a 250-digit number that was successfully found when writing these lines.³³

The Shor algorithm’s primal resolution capability on a quantum computer leads to the breaking of any encryption process that owes its immunity to prime factorisation. But equally vulnerable are the procedures based on discrete logarithm – a quantum algorithm has also been created to solve this problem. The methods that apply them are, therefore, not considered safe in the future. In contrast, for others, security can be retained in the post-quantum age by changing parameters (increasing key length).

The NIST report summarises the quantum computer’s impact on the most commonly used methods.³⁴

Table 5: Cryptographic algorithms and their impact

Algorithm	Applicability	Security sustainability
AES	Encryption	Stays secure with a larger key
SHA-2, SHA3	Hash	Longer output required
RSA	Digital signature, key negotiation	Unsafe
ECDSA, ECDH	Digital signature, key exchange	Unsafe
DSA	Digital signature, key exchange	Unsafe

Source: Compiled by the author based on Shor, ‘Polynomial’.

Quantum computers are primarily a threat to asymmetric encryption protocols, so attackers are expected to attack applications based on them. For protection, some parts of the X509 certificates, IKEv2, TLS, S/MIME and SSH protocols need to be modified. The widely used SSL and TLS protocols will no longer be reliable. This will affect almost all browser-based applications currently in use, even banking applications. Depending on the method used, encrypted media, VPN channels and remote login methods can be compromised with a quantum machine. Loss of SHA security can also compromise blockchain technology to have a serious impact on some cryptocurrencies. The SHA-256 hash algorithm used in the mining of Bitcoin may be at risk. The ability to retroactively change the blockchain guarantees creating a new chain and the loss of the Bitcoin owner’s money under certain conditions. RSA’s 2048-bit encryption breach is predicted by some sources within 8 hours.³⁵

³² Each compound number can be broken down into the product of a few prime numbers (for example, 15 to 5 and 3), this is the prime factor resolution. Prime numbers are numbers that cannot be divided by whole numbers other than 1 and themselves without residue, and it has been proven in ancient times that there are an infinite number of them.

³³ Source: <https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html>

³⁴ Lily Chen et al., *Report on Post-Quantum Cryptography* (Gaithersburg: National Institute of Standards and Technology, 2016).

³⁵ Steve Jurvetson, ‘How a quantum computer could break 2048-bit RSA encryption in 8 hours’, *MIT Technology Review*, 30 May 2019.

In addition to extending the currently used algorithms, the development of new Q-algorithms has also begun. The NIST Post Quantum Cryptography Project³⁶ is investigating a number of new procedures. It currently includes 17 quantum secure algorithms that implement encryption and 9 digital signatures.³⁷

Quantum computers are not required for quantum-safe algorithms to work, they can be used on traditional machines and can be developed in two different ways. The simpler procedure is the extension, which makes the current algorithms secure, if possible. The essence of these solutions is most often to increase the key sizes. Because of this, the number of possible permutations increases dramatically, making it an unsolvable task for the quantum machine, as well. This procedure can be successfully applied in the case of AES, but is unsuitable to improve RSA or DSA; therefore, they should be replaced by other procedures in the future.

In order to be able to change these procedures as well, the development of completely new procedures has also begun. Encryption procedures that are also indecipherable for quantum machines are called post-quantum or simply Q-algorithms. The NIST Post Quantum Cryptography Project³⁸ is exploring a number of new methods that currently include quantum secure algorithms that implement 17 encryptions and 9 digital signatures.³⁹ Lattice-based cryptography is based on complex math equations, these algorithms are very effective in creating new cryptographic methods, which are not able to break even with a quantum computer. Another effective cryptographic algorithm is the supersingular isogeny key exchange, which uses 2,688-bit long public keys. Ultimately, a quantum computer must also be used to test the new algorithms, so a collaboration between government and business was initiated under the coordination of NIST. The first draft standards are expected to be available by 2022, which will define the basics of defence against post-quantum algorithms.

The practical implementation of the algorithms has also started. The New Hope algorithm aims to replace the TLS algorithm in the world of quantum machines. Google has implemented this under the name Combined Elliptic-Curve and Post-Quantum (CECPQ) in the Canary version of Chrome,⁴⁰ although this is currently only available on an experimental basis, but can now be used in some services. DigiCert has developed software used to generate post-quantum cryptographic (PQC) hybrid certificates that includes a quantum-safe algorithm in addition to the traditional cryptographic procedure for backward compatibility.

DigiCert's solution makes one of the biggest difficulties clear: in addition to the very long time it takes to develop, standardise and implement cryptographic protocols, it takes even more time to get out of existing systems, so each of the old elements present in existing systems can be a vulnerability.

³⁶ See <https://csrc.nist.gov/projects/post-quantum-cryptography>

³⁷ See <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions>

³⁸ See <https://csrc.nist.gov/projects/post-quantum-cryptography>

³⁹ See www.google.com/chrome/canary

⁴⁰ See www.google.com/chrome/canary

Quantum internet

The quantum Internet uses one of the quantum phenomena to transmit information and uses quantum computing algorithms to encrypt it. However, quantum cryptography differs from traditional cryptography not only in the strength of encryption. Because the fact of the measurement itself causes irreversible changes in the quantum process, an attacker could be intercepted as soon as he peeks in the communication process.

The scientific findings of the quantum Internet are also contradictory, stemming from a professional debate between Bohr and Einstein. The operation of the quantum internet is based on the phenomenon of 'spooky action at a distance' created by Einstein. The essence of this is that the changes of the particles in quantum entanglement occur in parallel regardless of the distance between them. The existence of the phenomenon has been proven on several occasions experimentally, but serious professional debates have arisen over the question of whether the speed of communication between two particles in contact can exceed the speed of light. Although the paradigm of Einsteinian physics states that it is impossible, there is nonetheless research that does not rule this out. One U.S. Government report mentions investigating the compliance of black holes with wormholes.⁴¹

Many countries provide a vast amount of money for the development of quantum computers, as a truly efficient application requires a significantly larger number of qubits than it does today. It is almost impossible to predict the extent of development, but it can be said that Moore's law to increase the number of qubits was not fulfilled. The main difficulty is to minimise the number of errors; a breakthrough has not yet been achieved in this area. The biggest question in technological advances, then, is not whether a quantum computer works, but to what extent it can be scaled. In fact, the answer to this question indicates the danger posed by the proliferation of quantum machines to current informatics.

Conclusions

Cryptographic procedures can essentially ensure communication between modern IT devices, ensuring the confidentiality and integrity of data. In addition to offensive and defensive military equipment, economic and public organisations, and critical infrastructures, procedures are used in accordance with approximately the same principles for the civil sector.

The hacking of encryption procedures and the development of new procedures were typical of all ages. Today, the algorithms used in the civil sphere are also strong enough to be impossible for state cyber organisations to decipher. Some countries use backdoor-based solutions in technical devices or algorithms, while others make it impossible to access network services in other countries. Although there is no mathematical way to decrypt encrypted data, there are a number of solutions that will ultimately ensure that the

⁴¹ Executive Office of the President of the United States, *Quantum Frontiers Report on Community Input to the Nation's Strategy for Quantum Information Science* (Washington: White House National Quantum Coordination Office, 2020), 25.

contents of the encrypted data are known. A well-known solution for this is the application of brute force methods for which the necessary infrastructure is widely available.

Data that gets out of data breaches is often encrypted, so it is essential to decode it, for which, in most cases, brute force methods are obviously used. With a higher-value VGA card and a simple office PC, I proved that a university employee password database could be decrypted with success above 20 per cent. Email and password pairs available on the Darknet may have affected university access by less than 1 per cent.

The principles of quantum computing go back to the 1980s, and over the past forty years, algorithms have been developed that can work on these machines. Since a functioning quantum computer has not been built in recent years, these have remained only theoretical possibilities. However, the emergence of working machines requires analysis, protection, or rethinking of existing algorithms to ensure the security of protection procedures. Cryptographic methods based on factorisation or discrete logarithm have become crackable with the construction of the quantum computer. Since the most commonly used algorithms, RSA and DSA, are based on factorisation, they should be replaced by other procedures in critical applications. As a first step, they should be tested and, if necessary, planned for replacement. It is essential to design controls that guarantee that the introduction of new equipment considers the possibility of the appearance of a working quantum machine. Also, the quantum computer's impact in other possible areas should be assessed, and protective procedures should be set up to respond to the challenge it faces, taking into account the principle of proportionality.

References

- Barrett, Daniel J, Richard E Silverman and Robert G Barnes, *SSH, The Secure Shell: The Definitive Guide*. Sebastopol: O'Reilly, 2001.
- Bitport, 'A titkosítás tiltása veszélyes', 30 March 2016. Online: <https://bitport.hu/a-titkositas-tiltasa-veszelyes>
- Chen, Lily et al., *Report on Post-Quantum Cryptography*. Gaithersburg: National Institute of Standards and Technology, 2016.
- Choi, Charles Q, 'IEEE Spectrum', *IEEE Spectrum*, 21 May 2020. Online: <https://spectrum.ieee.org/tech-talk/computing/hardware/qubit-supremacy>
- Executive Office of the President of the United States, *Quantum Frontiers Report on Community Input to the Nation's Strategy for Quantum Information Science*. Washington: White House National Quantum Coordination Office, 2020, 25.
- Fedorov, Aleksey K, Evgeniy O Kiktenko and Alexander I Lvovsky, 'Quantum computers put blockchain security at risk'. *Nature* 563, no 22 (2018), 465–467. Online: <https://doi.org/10.1038/d41586-018-07449-z>
- Forces.net, 'The First Man To Storm A Nazi U-Boat And Seize An Enigma Machine', 06 January 2016. Online: www.forces.net/services/navy/first-man-storm-nazi-u-boat-and-seize-enigma-machine

- Huszár, Péter, 'Ukraina közösségi finanszírozású, katonai célokat szolgáló oktokoptereinek elemzése'. *Hadmérnök* 14, no 2 (2019), 34–43. Online: <https://doi.org/10.32567/hm.2019.2.3>
- Jurvetson, Steve, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours'. *MIT Technology Review*, 30 May 2019. Online: www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours
- Klima, Richard E and Neil P Sigmon, *Cryptology: Classical and Modern*. Chapman and Hall/CRC Press, 2018. Online: <https://doi.org/10.1201/9781315170664>
- Knuth, Donald E, *The Art of Computer Programming*. Boston: Addison-Wesley, 1973.
- PA Media, 'UK has mounted covert attacks against Russian leadership, says ex-mandarin'. *The Guardian*, 24 October 2020. Online: www.theguardian.com/technology/2020/oct/24/uk-has-mounted-covert-attacks-against-russian-leadership-says-ex-mandarin
- Piodi, Franco and Iolanda Mombelli, *The ECHELON Affair*. Luxembourg: European Parliament, 2014.
- Shor, Peter W, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer'. *Society for Industrial and Applied Mathematics* 26, no 5 (1997), 1484–1509. Online: <https://doi.org/10.1137/s0097539795293172>
- Vanhoef, Mathy and Frank Piessens, 'Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2', *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, October 2017, 1313–1328. Online: <https://doi.org/10.1145/3133956.3134027>

The Impact of the Covid Pandemic on Security and the Military: Civil-Military Cooperation in the Fight against the Covid Pandemic

József PADÁNYI¹ – József ONDRÉK²

A global health crisis can have long lasting effects on many areas of life, and the military is not exempt of its effects either. This article aims to highlight the possible usage of the military in various forms of emergency situations, especially in the case of the current coronavirus pandemic, particularly focusing on cooperation based on partnerships, while also highlighting the effects the Covid-19 epidemic had on the military. Civil-military cooperation (CIMIC) is a cornerstone of military operations these days, and its positive effects on military operations, especially in the struggle against the pandemic are also detailed. This study is based on the events and experiences of the first seven months since the outbreak of the Covid pandemic.

Keywords: CIMIC, Covid, pandemic, cooperation, military

Introduction

This article aims to highlight the possible usage of the military in various forms of emergency situations (currently, in the case of the coronavirus pandemic), particularly focusing on cooperation based on partnerships, while also highlighting the effects the Covid-19 epidemic had on the military. The study is based on the events and experiences of the first seven months since the outbreak of the Covid pandemic.

The deployment of the military in crises did not start with the coronavirus at all. Soldiers have already proven their preparedness in countless disaster management situations, let those be either natural, or industrial occurrences. The same may be stated also about international peace support or peacekeeping operations from Kosovo and Bosnia and Herzegovina to Cyprus. The fact that military forces are both able and ready to fulfil such tasks is neither questioned nor has it been doubted. This current research in relation

¹ Professor, University of Public Service Department of Military Strategy, Faculty of Military Science and Officer Training; e-mail: padanyi.jozsef@uni-nke.hu

² PhD, University of Public Service Department of Military Strategy, Faculty of Military Science and Officer Training; e-mail: ondrek.jozsef@uni-nke.hu

to the novel virus shows that, where they treated this threat with an appropriate level of seriousness, military forces were among the very first to be deployed in response to it.

It is thus worth asking why the deployment of the military is so efficient in such cases. The answer to that question lies in previous experiences.

The military operates in a strict order, where tasks and responsibilities are clearly outlined, while it is also equipped with an appropriate leadership structure to control this complex system. This allows for a rapid and efficient mobilisation, the involvement of professional experts in a fairly limited amount of time and adequate reserves.

Another advantage of using the military in such cases is that they are already equipped with special tools and professional knowledge, while they operate their own lines of logistics, as well. Thus, the supply of the entire staff involved in the tasks (including food, transportation, medical support, rest, communication, shifts) is there, it does not place a burden on other organisations involved in disaster management at the same time and location.

Last but not least, the discipline of military personnel is a determining factor that contributes to a higher level of efficiency.

Although mentioned less frequently, but the appearance of soldiers also has a positive psychological effect, as they represent security in the eyes of most of the population. They radiate a sense of support, care and attention, which raises the levels of security among the citizens while also improving their determination. Based on first hand personal experiences, it can be stated that if a uniform clad person appears in a crisis management situation, the trust of the populace in the successful management raises. The questions of civil-military cooperation – let it be in the course of wars or crisis management operations, such as military responsibilities during the coronavirus pandemic – receive increasing attention and importance these days.

The principles of civil-military cooperation

Military operations never take place in a vacuum. Both during the preparatory phase and the actual execution of operations, military planners pay particular attention to the civilian populace, to non-governmental organisations, and to all those other civilian actors who could in any shape or form affect the success of the operation. It is clear to see that the level of who receives this particular attention the most changes with the different type of missions. Cooperation with the civilian populace, and fulfilling their needs is significantly different in a wartime environment than in the case of a flood prevention operation. Equally, the room for manoeuvre for NGO-s is much different in a migration crisis than in an armed conflict. It is not among the aims of this study to delve into the particularities and differences of these scenarios. The aim is to draw up a uniformly accepted set of principles, tasks, cooperation possibilities and necessities that have already been tested and proven in practice.

Civil-Military Cooperation (CIMIC) is viewed today as a form of support for the military leader in aiding that person making the best possible decision. A prerequisite of this is that, during the course of the operation, a continuous, mutually respectful cooperation must

be established with the local populace and their leaders, with civilian governmental and non-governmental organisations, law enforcement organisations, civil protection services, religious organisations, the leading figures of the private sector, national authorities, and last but not least, with the various international organisations present. Therefore, the roles of the CIMIC staff, as part of the greater military organisation, may be classified into these three areas:

1. supporting the work of the military leadership (commander)
2. supporting the civilian sector
3. maintaining a continuous cooperation between the military and the NGO-s

In the long line of partners, the most important is naturally the civilian populace, since maintaining a balanced relationship with the local communities guarantees the establishment and maintenance of a secure environment. It should also be accepted that, in most cases, the military is not the most significant actor in a crisis response operation.

It is thus also worth looking a little back in time to see how military science writers and soldiers approached factors influencing military operations in the past.

The importance of the operational environment – and in particular of the population – had been highlighted by the earliest of military science works. Numerous ancient Chinese classical works deal with this question. It was frequently stated point even in military science literature from the ancient Warring States period in China that wars needed to be won not only on the battlefield, but also in the hearts of the populace (including the general enemy populace and military personnel as well). Winning the hearts and minds of the people was an important element of contemporary Chinese military science and this concept is still frequently used these days.

Every well-trained military leader has recognised – either through compulsion or at their discretion – the importance of civil-military cooperation. Later on in history, as the circumstances of warfare changed, so did the framework for civil-military cooperation. Non-governmental organisations started to take part in CIMIC, the self-organisation power of the populace has increased while the role of the press and the media has become even stronger. The military force entering a crisis area has to pay more attention to creating the conditions for political, economic, humanitarian development, laying the foundations for social and legal stability not by force, but rather by creating and maintaining a secure environment. This shift in approach was well emphasised by then General Eisenhower near the end of World War II when he exclaimed: ‘The sooner I can get rid of all these questions that are outside the military in scope, the happier I will be! Sometimes I think I live ten years each week, of which at least nine are absorbed in political and economic matters.’³

Following the end of the war in the Balkans, peacekeeping operations have once again raised the importance of civil-military cooperation to a new level. ‘In November (1995),

³ Robert M Gates, ‘Secretary of Defense speech, Brookings Institution Dinner (Washington, D.C.)’, *U.S. Department of Defense*, 21 July 2020.

we had never heard of CIMIC, we had no idea what you did [...] now we can't live without you', said Admiral Leighton W. Smith, the Commander of IFOR (Implementation Force).⁴

NATO has also realised the importance of CIMIC hence, and in 2007, decided to establish the NATO Civil-Military Cooperation Centre of Excellence. The aim of the Centre is to provide opportunity for its members to assess their CIMIC experience, and to share it through timely education and training.⁵

CIMIC principles will effectively guide commanders and NGOs provided that the following general requirements are met:⁶

1. Understanding and acknowledging the civil environment and civilian actors which includes, among others, data collection, analysis and evaluation. This way, military forces are able to define the cooperation framework in a credible, confident manner with as little hindrance as possible.
2. Understanding the aims, objectives, symbols and history of all non-military actors impacted. This act will unlock synergies in cooperation that will eventually strengthen the acceptance and respect of military forces.
3. Respecting others, being open, taking competent responsibility, demonstrating and applying the necessary skillset, that is, creating and maintaining credibility and authenticity are all required. Furthermore, these have to work on a mutual basis, they are not functional in a one-way relation.
4. Joint preparation and planning of tasks of common interest. Namely, defining the path to achieving the goal, clarifying joint efforts in time, including a possible division of labour and distribution of responsibilities.
5. Defining the order and organisational framework of the cooperation.

The consistent application of the aforementioned actions during the coronavirus pandemic has enabled the military to be able to support the civilian sector effectively without major roadblocks.

Specific tasks

Reviewing coronavirus related news, one can draw some generic conclusions. In the 42 countries that were examined for this study, military forces were mobilised in every state – to a varying degree but on the basis of similar principles – to solve certain tasks in the epidemic situation. Before analysing the Hungarian response to Covid-19, it is worth looking at some international examples, as well.

As it has been stated earlier, military forces are equipped with special tools and professional knowledge that can be well applied in crisis situations. In the fight against the coronavirus, their equipment was used for logistic activities in the air, on water and

⁴ William R Philips, 'Civil-Military Cooperation: Vital to Peace Implementation in Bosnia', *NATO Review* 46, no 1 (1998), 25.

⁵ More details can be found at www.cimic-coe.org/about-ccoe/sponsoring-nations

⁶ *CIMIC Handbook*, Civil-Military Cooperation, Centre of Excellence, 2020.

also on land. Several military aircraft were involved in the repatriation of citizens when civilian air traffic was no longer available. Thousands of people were able to return to their home country because their government sent military aircraft to pick up civilians who were stranded abroad. The various air forces were tirelessly delivering medical supplies and equipment to countries which experienced shortages of ventilators, medicines, PPE and disinfectants.

Furthermore, the military also used off-road vehicles (ORV) to supply hard-to-reach areas with food and medicine. For instance, the military used ORVs in Albania to help vulnerable mountain communities with supplies while in Austria, they assisted in the replenishment of shops. Portugal shows another example of CIMIC where military officers assisted homeless citizens during critical times.

In the United Kingdom (U.K.), 150 soldiers were trained and deployed to perform special road transport tasks (transporting oxygen, personal protective equipment and rescue equipment). Further tasks of these troops included the support of mobile testing sites and ambulance services, increasing medical capacity and building field hospitals.⁷

There have also been examples of Covid-patients being transported by the military. The German Air Force airlifted six coronavirus patients from Italy and later did the same in France to reduce the burden on their respective healthcare system.

U.K. military personnel – based on their previous engineering experiences and their existing tools and equipment – built a temporary hospital with a capacity of 4,000 beds in just nine days. In the United States, experts of the U.S. Army Corps of Engineers were also building dozens of hospitals across the country while U.S. Navy hospital ships were deployed at the most impacted coastal cities to relieve the burden on hospitals there.⁸

In South Korea, the coronavirus epicentres were effectively dissolved by experienced and well-equipped CBRN (chemical, biological, radiological, nuclear) units. In Spain, military officers were engaged in the decontamination and disinfection of critical infrastructure (ports, airports, train stations, healthcare facilities) and currently there are 2,500 soldiers who are fighting against the coronavirus in 172 cities.

Several countries have deployed their troops along with civilian authorities and police to monitor compliance with quarantine requirements. On the top of that, various tools were applied in the fight against Covid-19, such as joint patrols, drones, smart systems (mobile applications, contact and infection tracking).

Leadership and organisational skills are particularly valuable in such cases, and these are all required of military personnel anyway. Regarding the defensive measures in the U.K., one of the most significant element was the deployment of military planners who have supported the work of the local Coronavirus Task Forces.⁹

Increasing military presence in public areas helped to strengthen the confidence of the populace, which also affected the work of the police in a positive way. This strong presence also helped to maintain curfews, quarantines and similar restrictions. On a European level, the fight against the coronavirus has become more complicated due to the

⁷ 'Coronavirus: What The Military's Doing To Fight COVID-19', Forces.net, 15 August 2020.

⁸ 'USACE COVID-19 Response Efforts', *US Army Corps of Engineers Headquarters*, 21 July 2020.

⁹ Ibid.

simultaneous presence of the epidemic, closed borders and large number of refugees. For this reason, the military provided assistance in these situations as well. Austria mobilized 2,200 military personnel to support border guards in patrolling its borders. Controlling border crossing was one of the most critical activities that required military assistance in several countries, including the United States, Poland, Serbia, Bosnia and Herzegovina and Montenegro.¹⁰

The coronavirus has emerged with different intensity in each country, which – luckily – allowed the nations to mutually support each other in their defence against the virus. Military forces have also excelled in this area. Albania sent a medical team of 30 to Italy to help local doctors. With their military aircraft, Russia sent eight military medical teams, around one hundred virologists and epidemiologists with international experience, mobile disinfection systems as well as other medical equipment to Italy. Additionally, Russia also sent supply packages to the U.S. with its available aircraft. Poland deployed 15 Polish doctors and paramedics to a Lombard field hospital. Germany offered nearly 45 tons of medical equipment to Romania including 100,000 pieces of PPE. The supply was delivered by the Romanian Air Force. On the other hand, the aircraft of the Romanian Air Force flew both doctors and equipment to Milan from Bucharest to support Italy in its fight against Covid-19.¹¹

Although it may seem peculiar, but maintaining the mental health of the populace and enhancing their mood were also important tasks of the military that included public performances of military bands, making military museums available online, or organising tribute flights to recognise the tremendous job of healthcare workers.

The case of military medicine has to be mentioned too, since it was – and in many cases it is still – placed under double load. On the one hand, military medical personnel support their civilian counterparts in all possible ways. While on the other hand, they are fighting their own battles against the mass spread of the virus in the armed forces. Since soldiers are on the front lines in the fight against the virus, they are also especially vulnerable. Their protection, and stopping isolated cases of infection becoming mass occurrences, has become the most important tasks of military medicine. If medical personnel were to fail in this task, it would seriously jeopardise the ability of military organisations to fulfil their primary (military) roles.

The Hungarian Defence Forces in the struggle against the pandemic

Upon closer inspection of how the situation unfolded in Hungary, it is clear to see that the country had to face comparable challenges and provide similar answers as its neighbours.

¹⁰ Shawn Snow, '540 additional troops to deploy to U.S.–Mexico border over COVID-19 concerns', *Military Times*, 01 April 2020.

¹¹ 'Military assistance in the fight against COVID-19 in Europe – solidarity in action', *European Union External Action Service (EEAS)*, 12 May 2020.

On 11 March, the Hungarian Government announced Government Decree 41/2020 on the measures to be taken during the state of emergency declared for the prevention of the human epidemic endangering life and property and causing massive disease outbreaks, for the elimination of its consequences, and for the protection of the health and lives of Hungarian citizens.

According to its roles described in the Fundamental Law of Hungary, the Hungarian Defence Forces immediately joined the fight against the virus with all its capabilities, personnel and knowledge. On a daily basis, it meant the deployment of over two thousand soldiers and four hundred vehicles. The Defence Forces deployed pre-testing tents, and also participated in the closure and strengthening of the borders. Military Police patrolled in twelve garrison towns and controlled the compliance with curfew restrictions. Hungarian Defence Forces personnel guarded (and in fact, still guard) the warehouses where essential personal protection equipment are stored, including ten millions of masks, rubber gloves, cloaks and ventilators. There was a military officer at the head of 51 hospitals in 13 counties, coordinating prevention preparation, securing hospital beds, maintaining supplies and providing the required data. The so-called Hungarian Defence Forces Management Groups coordinated the operation of 105 companies during the emergency situation. Employing its biological and chemical defence capabilities, the HDF had disinfected 1,034 nursing homes.¹²

The Hungarian Defence Forces also participate in the economic protection action plan of the Government. With the introduction of a new, 'special voluntary reserve' service, the HDF is able to employ 3,000 people for up to one year. After this special period comes to a conclusion, these volunteers are going to have the opportunity to continue their military careers, albeit they are going to have to pass more rigorous requirements than before.¹³

Naturally, the virus did not spar Hungarian soldiers either, but fortunately, less than ten cases have been found so far by concluding more than 1,500 tests.¹⁴

In a crisis management situation, establishing the culture and the ways of cooperation are essential. While in many cases, this usually works instinctively, it is much better if one is prepared for such role in advance. CIMIC therefore is one of the most important elements of military support, as it serves exactly this purpose. It has established methods, systems and professional experts. Such special preparedness was received as an advantage during the defence against the coronavirus, when military personnel were sent to hospitals, onto the streets and to strategic corporations to do their respective duties there.

Altogether, it can be confidently stated that in the fight against the coronavirus, military forces have a determinative role all over the world. While it is also worth noting that most of the populace does not question the necessity of such actions and does not see these as part of a militarisation of everyday life. They mostly see that human and technical

¹² 'A hadsereg alkalmazása a koronavírus-járványban' [Deployment of the Military during the Coronavirus Epidemic], *Parlament.hu*, 27 April 2020.

¹³ 'Benkő Tibor: a honvédelemre, a biztonságra mindig kiemelt figyelmet kell fordítani' [Tibor Benkő: Particular attention has to be paid to homeland defence and security at all times], *Magyar Honvédség Online*, 14 July 2020.

¹⁴ 'Kulcsfontosságú a honvédség szerepe a koronavírus elleni védekezésben' [Defence forces are vital in the defence against the coronavirus]. *Háború Művészete*, 21 April 2020.

resources alike, do what their duty is: they help in establishing and maintaining a secure environment.

The pandemic had a significant impact on the general, overall security of society. One of these impacts in the future could be the re-emergence or intensification of bio-terrorism. The experiences of these last few months have steered the mind of the general public into contemplating such cases, and thoughts like these actually fuel actions of a similar kind. Terrorism, in most cases, is not devastating on its own, but its destructive impact lies in the effect it has on society. The wildfire-like spread of Covid-19 has naturally frightened most people, and with it, their belief in the established order started wavering, which is exactly the same effect an act of terrorism wants to achieve. Cynically speaking, it is possible to say that the pandemic provided those radical groups with an idea, which are interested in the appearance of weak states.

For example, in Egypt, the Muslim Brotherhood has called upon its members to go out and spread the virus, preferably to soldiers and government officials, thereby weakening their organisations. One could ask, if this may be considered a new form of bio-terrorism or not?

As another example, the Islamic State called upon its supporters to use the chinks in the armour of security systems overwhelmed by the pandemic and attack there.¹⁵

In terms of security, one should also consider the response of organised crime to the disruption caused by the coronavirus. It is not strictly the responsibility of the military, however, numerous countries have strengthened their law enforcement with military officers, since police forces have been regrouped to fight against local crimes.

During this period, several examples highlight that organised crime groups have been particularly active in money laundering, organising mass migration and in the procurement and distribution of protective equipment.¹⁶

Additionally, one must also stress the impact of coronavirus on cybersecurity in the global security environment. With the outbreak of the virus, the number of cybercrimes and network threats has increased significantly. The spread of false information, frauds related to non-existent companies and fake adverts of non-existent medical products have caused financial loss and moral damage in many households globally. As a result of this phenomenon, several countries – for instance Romania and the United Kingdom – have requested the assistance of military personnel specialised in cybersecurity to respond to the threats and prevent cyberattacks.¹⁷

Interesting connections may be brought to light, when one looks at the publicity of pandemic related news. The forces and tools involved in the struggle against the pandemic as well as the particular action plans were communicated differently in each country. Western European countries in general provide more clarity when communicating information on the pandemic and its impacts as well as on informing the population about the response plans. German and Austrian officers make nearly every information publicly

¹⁵ Julie Coleman, 'The Impact of Coronavirus on Terrorism in the Sahel', *International Centre for Counter-terrorism – The Hague*, 16 April 2020.

¹⁶ Jason Eligh, 'Crisis and Opportunity: Impacts of the coronavirus pandemic on illicit drug markets', *Global Initiative*, 13 May 2020.

¹⁷ 'Kulcsfontosságú a honvédség szerepe'.

available. As one moves more towards Eastern Europe, it can be noticed that nations tend to limit the amount of public information. This approach is not necessarily wrong as it may have several security benefits. From a military aspect, if a country loses, even temporarily, a significant part of its military capabilities, it may not want to announce this information to the populace.

The impact of the pandemic on military forces

In many countries, it has become a practice to postpone the enlistment of conscripts and reserves, keeping instead the already serving personnel in active duty. In some cases, those falling under compulsory conscription were not enlisted yet, in case the already serving personnel got infected. Training exercises were also modified accordingly. All this was leading to instances where combat effectiveness and combat readiness decreased. This is reinforced by a budgetary decision that reallocates – entirely or partially – the military development budget to support defence spending against the virus. Croatia has decreased its defence budget by 25 million Euros, and South Korea has also decided on a similar scale budget reduction.¹⁸

As the coronavirus infection knows no barriers, the military personnel are exposed to it as well, thus directly affecting military security. The daily lives of UN, EU and French peacekeeping missions in Mali were seriously affected by the emergence of the epidemic within their ranks. Joint forces (mainly German, Spanish and Czech) were withdrawn on a daily basis, and the staff rotation system of the French-lead Barkhane mission has also been changed as an answer to the local health crisis.¹⁹ In one of its statements, an official of the French Ministry of Armed Forces estimated that around 4,000 individuals have contracted the virus in several organisations operating under the Ministry. The pandemic even reached the French aircraft carrier Charles de Gaulle (R91) where more than 50 crew members have tested positive. As a result of the outbreak, the deployment of the carrier was stopped and it had to return to its home port in Toulon, France.

The U.S. Navy had to face a similar case when one in five sailors (1,000 people) were tested positive for Covid-19 on the aircraft carrier USS Theodore Roosevelt (CVN-71). In order to isolate the spread of the virus, the Nimitz-class aircraft carrier ended its deployment and disembarked in San Diego.²⁰

As another example, Israel is considering the coronavirus pandemic a serious security threat since it drastically reduced its defence capabilities. Securing supplies for the populace and maintaining order have required a significant load on the staff and capacities of their security forces, including the Israel Defense Forces, the National Security Services and the Israel Police.

¹⁸ 'COVID-19 to impact defence budgets: Poll', *Army Technology*, 22 May 2020.

¹⁹ Ibid.

²⁰ Monica Garske, 'USS Roosevelt, stricken by COVID-19 outbreak in March, returns from deployment', *NBC San Diego*, 09 July 2020.

Even the Mossad (the Israeli intelligence agency) was involved in the procurement of critical personal protective equipment (experiences show that in some cases the already purchased equipment could not reach its destination as it had been previously seized by the states the consignment was passing through). In this unprecedented situation, every solution and method seemed appealing and unprohibited. In Israel, attempts were made to mitigate the increased threat to soldiers by reducing the number of exercises, which at the same time weakened the preparedness of the armed forces.

Soldiers returning from foreign missions also pose a serious risk in terms of the national military force and protection against the spread of the virus. For instance, Polish soldiers on peacekeeping mission in Afghanistan were flown back to Poland, however, 99 individuals contracted the coronavirus right before their departure. As confirmed by the Polish Chief of Staff, the majority of the infected soldiers showed no symptoms, which means that, without a timely diagnosis, they could have easily been an even greater risk.²¹

NATO's response to Covid-19

When fighting pandemics, one may not think of NATO as the first international organisation to be involved. However, the North Atlantic Treaty Organization has reacted fast to the new global situation and has used and still uses all its available tools to assist member states and partner countries in their defence against the virus. NATO troops have been engaged in various areas and their assigned tasks included the effective coordination of supply chain logistics, transporting essential medical staff, medicine and other protective equipment and supplies, supporting civil-military programs that study the virus, providing strategic airlift to evacuate and repatriate citizens as well as disaster relief.²²

NATO and disaster management

The role of the 24/7 operating Euro-Atlantic Disaster Response Coordination Centre (EADRCC), as the main emergency response mechanism of NATO, is of key importance in the battle against the pandemic. Incoming requests are managed centrally and distributed either to one of the Allied countries (for example, the Czech Republic, Germany or Turkey) or to their partners who then provide assistance in disinfecting hospitals or transporting supplies. For instance, Bosnia and Herzegovina received a large amount of thermometers, 5,000 masks, protective gloves, blankets and disinfectant. Another great example for international cooperation goes back to 9 April, when Luxembourg donated 1,440 kg of Tyvek material for Spain so that they could produce protective equipment for their essential healthcare workers.²³

²¹ 'Poles stranded in Afghanistan return to Poland by military plane', *The First News*, 05 May 2020.

²² Attila Mesterházy, 'The Role of NATO's Armed Forces in the COVID-19 Pandemic', *NATO Parliamentary Assembly*, 18 June 2020.

²³ 'NATO's Response to the COVID-19 Pandemic', *North Atlantic Treaty Organization*, 14 April 2020.

Also in April, the Czech Republic demonstrated another great example of mutual support when it sent supplies to the Balkans. As per the request of North Macedonia, the 242nd Transport and Special Squadron of the Czech Air Force Command transported 1,000,000 face masks to the country.²⁴ In addition to transportation activities, NATO has launched a scientific research project within the Science for Peace and Security Programme that aims to develop a new tool capable of diagnosing the coronavirus infection rapidly and accurately.²⁵

NATO and its strategic airlift

Within the framework of its Strategic Airlift International Solution (SALIS) program, NATO is committed to reserve transportation for oversized military equipment in civilian aviation in order to provide sufficient and timely air transport capacity for the deployment of forces as well as for the realisation of individual long-distance national cargo operations.²⁶ Within the framework of the program, Turkey was able to deliver essential medical supply to the U.K. while the U.S. Air Force distributed more than 15,000 kg of supplies across Italy.²⁷

Parallel to the SALIS program, the Strategic Airlift Capability of NATO has also played a key role in the international fight against the pandemic. Ten NATO member states and two partner countries jointly operate three Boeing C-17 Globemaster III aircraft that are home based at Pápa Air Base, Hungary.²⁸ The operating nations share the costs based on flight hours and use the three heavy military cargo aircraft for national defence or, in the time of a global pandemic, for humanitarian relief missions.²⁹

The NATO–EU cooperation

Both the NATO and the European Union have quickly recognised that a joint response and strategy would be critical to stop the spread of the virus and mitigate its impact on societies. NATO and EU representatives have highlighted two principal areas of concern for their cooperation: military mobility and countering disinformation.

The Alliance has been considering the development of military mobility as one of its top priority as outdated infrastructure and bureaucratic procedures often hinder member

²⁴ 'Coronavirus response: Czech Republic delivers assistance to North Macedonia', *North Atlantic Treaty Organization*, 10 April 2020.

²⁵ Tania Lațici, 'NATO's response in the fight against coronavirus', *European Parliamentary Research Service*, June 2020.

²⁶ Tamás Nemes, 'A NATO Támogató és Beszerzési Ügynökségének felépítése, feladatrendszere és együttműködése a Magyar Honvédséggel' [The NATO Support and Procurement Agency, its structure, roles and cooperation with the Hungarian Defense Forces], *Katonai Logisztika 2* (2016), 14.

²⁷ Tania Lațici, 'NATO's response in the fight against coronavirus'.

²⁸ Member states: Bulgaria, Estonia, Hungary, Lithuania, the Netherlands, Norway, Poland, Romania, Slovenia and the United States. Partner states: Finland, Sweden.

²⁹ 'The Strategic Airlift Capability – The Essential Facts', *Strategic Airlift Capability*, 21 July 2020.

states to move their forces quickly across Europe both in peacetime, crisis and conflict. In March 2020, the NATO Secretary General and EU defence ministers have agreed that both organisations play an important role in building the necessary infrastructure and legal framework, which would enable the quick movement of military forces in the region.³⁰

Regarding disinformation, the coronavirus pandemic has become the first global health event where digital platforms (mainly social media) can largely impact the perception and knowledge on the virus by the population. Due to the large-scale digitisation, its geopolitical impact has also been increasing. Alongside the available real information on Covid-19, disinformation campaigns have also emerged that aim to question the provenance, spread and symptoms of the disease. For this reason, together with the EU, NATO strives to identify, track and disclose these disinformation cases.³¹

Conclusions

The coronavirus outbreak and its intensity have given new approaches and opened new dimensions for civil-military cooperation. It has become clear that military forces are able to provide human and technical resources whose capabilities cannot be ignored in such a global environment. Special expertise, specific equipment and logistical background are the main enablers of an effective defence against the virus.

For many years, the military has been consciously building the theoretical and practical framework for civil-military cooperation, let it be disaster prevention, administrative support or specific circumstances of peacekeeping operations. In the past few years, NATO has established its own organisation dedicated to civil-military cooperation, while further national CIMIC centres, units and subunits are also being formed. Concurrent to these changes, the theoretical and regulatory background and the procession of experiences are constantly evolving. These provide a solid basis for an effective and smooth deployment of military forces in the fight against the epidemic.

The pandemic has also largely impacted the military personnel and missions of the armed forces, thus indirectly, military security as well. By its nature, military forces operate in closed communities, hence they are more exposed to infection due to the rapid spread of Covid-19. Considering the lack of diligence and prevention, the emerging epidemic may jeopardise entire units, subunits or even naval ships which directly raise national security issues.

Another direct impact of the current situation on military forces may be a reduced effectiveness of operations due to the low number of soldiers available (either because of illness or preventive restrictions). Such a situation would provide enemy forces with more room to operate.

The pandemic has also shown that leveraging military expertise and using special tools for different purposes also enhance the knowledge of teams that have been only put in the

³⁰ Mesterházy, 'The Role of NATO's Armed Forces'.

³¹ 'Speech of Vice President Věra Jourová on countering disinformation amid COVID-19. From pandemic to infodemic', *European Commission*, 04 June 2020.

spotlight during combat operations so far (for example, CBRN defence). Therefore, due to the change of focus points in the actual fight or, in a broader sense, in military operations, certain areas may receive less attention, but in the development of new equipment one has to always consider the requirements of multi-functionality.

The recognition and acknowledgement of military forces have been improving as a result of their professional, often self-sacrificing service during the pandemic. Although, at first there were voices among the population that feared the militarisation of a given society, by today these concerns have been mostly eased.


References

- ‘A hadsereg alkalmazása a koronavírus-járványban’ [Deployment of the Military during the Coronavirus Epidemic]. *Parlament.hu*, 27 April 2020. Online: www.parlament.hu/documents/10181/4464848/Infojegyzet_2020_23_hadsereg_koronavirus-jarvanyban.pdf/b6ad6867-0d0e-08c9-6462-b3bf336cff07?t=1587974484535
- ‘Benkő Tibor: a honvédelemre, a biztonságra mindig kiemelt figyelmet kell fordítani’ [Tibor Benkő: Particular attention has to be paid to homeland defence and security at all times]. *Magyar Honvédség Online*, 14 July 2020. Online: <https://honvedelem.hu/hirek/hazai-hirek/benko-tibor-a-honvedelemre-a-biztonsagra-mindig-kiemelt-figyelmet-kell-forditani.html>
- Coleman, Julie, ‘The Impact of Coronavirus on Terrorism in the Sahel’. *International Centre for Counter-terrorism – The Hague*, 16 April 2020. Online: <https://icct.nl/publication/the-impact-of-coronavirus-on-terrorism-in-the-sahel/>
- ‘Coronavirus response: Czech Republic delivers assistance to North Macedonia’. *North Atlantic Treaty Organization*, 10 April 2020. Online: www.nato.int/cps/en/natohq/news_175070.htm
- ‘Coronavirus: What The Military’s Doing To Fight COVID-19’. *Forces.net*, 15 August 2020. Online: www.forces.net/news/coronavirus-how-military-helping
- ‘COVID-19 to impact defence budgets: Poll’. *Army Technology*, 22 May 2020. Online: www.army-technology.com/news/covid-19-to-impact-defence-budgets/
- CIMIC Handbook*, Civil-Military Cooperation, Centre of Excellence, 2020. Online: www.cimic-coe.org/products/conceptual-design/downloads/ccoe-publications/field-handbook/
- Eligh, Jason, ‘Crisis and Opportunity: Impacts of the coronavirus pandemic on illicit drug markets’. *Global Initiative*, 13 May 2020. Online: <https://globalinitiative.net/coronavirus-illicit-drug-markets/>
- Garske, Monica, ‘USS Roosevelt, stricken by COVID-19 outbreak in March, returns from deployment’. *NBC San Diego*, 09 July 2020. Online: www.nbcsandiego.com/news/local/uss-roosevelt-stricken-by-covid-19-outbreak-in-march-returns-from-deployment/2361996/
- Gates, Robert M, ‘Secretary of Defense speech, Brookings Institution Dinner (Washington, D.C.)’. *U.S. Department of Defense*, 21 July 2020. Online: <https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1237>
- ‘Kulcsfontosságú a honvédség szerepe a koronavírus elleni védekezésben’ [Defence forces are vital in the defence against the coronavirus]. *Háború Művészete*, 21 April 2020. Online:

www.haborumuveszete.hu/egyeb-hirek/kulcsfontossagu-a-honvedseg-szerepe-a-koronavirus-elleni-vedekezesben

- Lažiči, Tania, 'NATO's response in the fight against coronavirus'. *European Parliamentary Research Service*, June 2020. Online: [www.europarl.europa.eu/RegData/etudes/ATAG/2020/651955/EPRS_ATA\(2020\)651955_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2020/651955/EPRS_ATA(2020)651955_EN.pdf)
- Mesterházy, Attila, 'The Role of NATO's Armed Forces in the COVID-19 Pandemic'. *NATO Parliamentary Assembly*, 18 June 2020. Online: www.nato-pa.int/download-file?filename=sites/default/files/2020-06/091%20DSC%2020%20E%20-%20COVID-19%20SPECIAL%20REPORT_1.pdf
- 'Military assistance in the fight against COVID-19 in Europe – solidarity in action'. *European Union External Action Service (EEAS)*, 12 May 2020. Online: <https://eeas.europa.eu/headquarters/headquarters-homepage/79159/military-assistance-fight-against-covid-19-europe-%E2%80%93-solidarity-action>
- 'NATO's Response to the COVID-19 Pandemic'. *North Atlantic Treaty Organization*, 14 April 2020. Online: www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/200401-factsheet-COVID-19_en.pdf
- Nemes, Tamás, 'A NATO Támogató és Beszerzési Ügynökségének felépítése, feladatrendszere és együttműködése a Magyar Honvédséggel' [The NATO Support and Procurement Agency, its structure, roles and cooperation with the Hungarian Defence Forces]. *Katonai Logisztika* 2 (2016), 14.
- Philips, William R, 'Civil-Military Cooperation: Vital to Peace Implementation in Bosnia'. *NATO Review* 46, no 1 (1998), 22–25.
- 'Poles stranded in Afghanistan return to Poland by military plane'. *The First News*, 05 May 2020. Online: www.thefirstnews.com/article/poles-stranded-in-afghanistan-return-to-poland-by-military-plane-12465
- Snow, Shawn, '540 additional troops to deploy to U.S.–Mexico border over COVID-19 concerns'. *Military Times*, 01 April 2020. Online: www.militarytimes.com/news/coronavirus/2020/04/01/540-additional-troops-to-deploy-to-us-mexico-border-over-covid-19-concerns/
- 'Speech of Vice President Věra Jourová on countering disinformation amid COVID-19. From pandemic to infodemic'. *European Commission*, 04 June 2020. Online: https://ec.europa.eu/commission/presscorner/detail/it/speech_20_1000
- 'The Strategic Airlift Capability – The Essential Facts'. *Strategic Airlift Capability*, 21 July 2020. Online: www.sacprogram.org/en/Pages/default.aspx
- 'USACE COVID-19 Response Efforts'. *US Army Corps of Engineers Headquarters*, 21 July 2020. Online: www.usace.army.mil/coronavirus/

The Role of the NATO Support and Procurement Agency in Support to Operations

György GULYÁS¹ – Árpád POHL² 

It is a basic requirement of the nations participating in multinational operations that the necessary resources be available at the required place and time, in the determined quality and quantity with optimal costs. In all of this, the Contractor Support to Operations, one of the pillars of the support to operations, has a more and more significant role. This method of support (besides the Host Nation Support) is destined for covering the gaps in the national military capabilities and capacities. It is indispensable these days to employ contractors for capitalising on their technological knowledge, as well as for achieving cost savings and a growth in the capabilities. The NATO Support and Procurement Agency (NSPA or Agency), the ‘contract integrator’ organisation of the NATO also support the NATO and the nations this way. In this article, the authors would like to introduce the operation of the NSPA and discuss the potential opportunities in its use.

Keywords: *contracted capabilities, contract, support to operations, multinational commercial solutions*

Introduction

Supporting the military operations through contracted solutions is a priority area of the logistic support. This form of the operation support is used very frequently during the peacekeeping missions, when achieving the goal makes the application of cost-effective solutions possible and when conservation of own resources is required. During the South Slavic war, the contracts came into view regarding the provision of support to the foreign troops stationed in Hungary, which also induced military researches. Endre Jávör, at Zrínyi Miklós National Defence University, defended his doctoral dissertation in 2002 with the title *Logistical support activities of the host nation in a multinational peacekeeping operation, with special regard to the implementation under private law contracts*. He examined the satisfaction of claims under the contracts from the point of view of the host

¹ Instructor, University of Public Service, Faculty of Military Science and Officer Training, Department of Supply, Finance and Military Traffic; e-mail: gulyas.gyorgy@uni-nke.hu

² PhD, Associate Professor, University of Public Service, Faculty of Military Science and Officer Training, Department of Supply, Finance and Military Traffic; e-mail: pohl.arpad@uni-nke.hu

nation. In the dissertation he proved the need to place the support of armed forces on a national economic basis and he also defined the relationship between the contract and the order in terms of the effectiveness of the services. An important result of his research was that he determined the requirements and contexts of the services provided under private law contracts based on the experiences.³ Tibor Balla, who examined the contracting support from the point of view of the Hungarian Armed Forces further studied the topic.⁴

An important feature of the peace operations is that those are conducted by multinational forces often on remote battlefields (for example Afghanistan). Only a few participating nations have the capabilities to carry out all support tasks and these functions would tie up significant military forces that even forces with a resource-rich logistical support system could not afford. In the NATO, the need for common support solutions can be traced from the beginning. In 1958, the North Atlantic Council (NAC) decided to establish the NATO Maintenance Supply Services Agency (NMSSA), whose responsibility at that time was limited to three major weapon systems.⁵

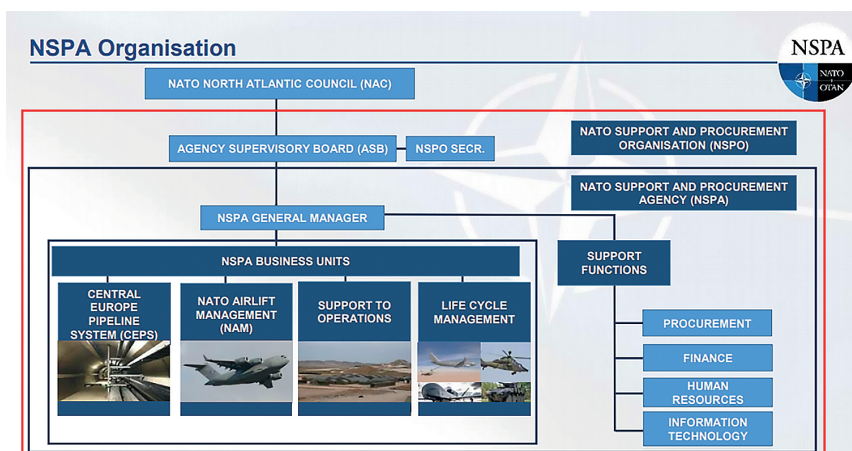


Figure 1: NSPA organisational structure

Source: NSPA/OLSP Basic Overview and Benefits (Agenda Item VIII), Presentation by Mr Dane Tynes, 23rd OLSP Committee Meeting, 20 October 2020.

The multinational logistics support solutions have gained ground and their effectiveness have been proven. According to the AJP-4(B), the NATO Agencies can support the military operations based on their competence.

³ Endre Jávör, *A befogadó ország logisztikai támogató tevékenysége többnemzetiségű békefenntartó hadműveletben, különös tekintettel a magánjogi szerződések alapján történő végrehajtásra* [Logistical support activities of the host nation in a multinational peacekeeping operation, with special regard to the implementation under private law contracts] (PhD dissertation, Budapest: Miklós Zrínyi National Defence University, 2002).

⁴ Tibor Balla, *Civil és katonai javak a szerződött logisztikai szolgáltatások tükrében* [Civilian and military goods in the light of the contracted logistical services] (PhD dissertation, Budapest: Miklós Zrínyi National Defence University, 2004).

⁵ Ibid.

The NATO Support and Procurement Organisation (NSPO) is established as a subordinate legal body of the North Atlantic Council (NAC). NSPO includes the Agency Supervisory Board (ASB) which is the governing body of the NSPA and all NATO nations are represented in it.

The mission of the NSPO is to provide responsive, effective and cost-efficient acquisition, including armaments procurement, logistics, operational and systems support and services to the Allies, NATO Military Authorities and partner nations, individually and collectively, in time of peace, crisis and war, in order to maximise the ability and flexibility of their armed forces, contingents, and other relevant organisations, within the guidance provided by the North Atlantic Council (NAC), to execute their core missions. The NSPO's executing body is the NATO Support and Procurement Agency.

In other words, NSPA is at the service of the NATO members and partner nations, equipment procurement and life cycle management, logistics services provider. The Agency is a 'no profit, no loss' organisation, without aiming the profit, covering the overheads, salaries and operational costs by the administrative fees of the established and managed contracted capabilities. The Agency is Customer Funded, Governed by the Agency Supervisory Board. It acts as an extension of the Armed Forces, covering the capability gaps missing from the military or national defence industry capabilities and capacities, but the NSPA does not compete with those.

The basic procurement activity of the Agency

A main objective of the NSPA is to obtain, through international competitive bidding, the most economical prices for materiel and services. The most economical proposal, which meets the technical and contractual requirements defined in the Request for Proposal (RFP), will normally be accepted.

To collect potential service providers, the NSPA uses a source file that includes commercial companies from the industry. The main purpose of the source file is to assist and facilitate the realisation of an effective source selection process making possible a successful competitive procurement.

NSPA normally acquires the materiel, supplies and services, required by its customers, through the international competitive bidding process from commercial sources. The procurement policy of the NSPA is based on the principles of integrity, transparency and equal treatment. However, under some very specific circumstances, the solicitation procedures can differ from the full and open international competitive bidding process. These circumstances are the following:

1. Sole Source: In case of existing only one known source which is capable of providing the required materiel, supplies and/or service.
2. Single Source: The procurement circumstances, as listed below, may justify the need to take into consideration only one source during the solicitation process, although other potential sources may also exist.

3. Urgency: These conditions can come into consideration when application of the full competitive bidding process would cause a delay in delivering the required materiel or services, defined by the customer as emergency requirements.
4. Low Value: When the extended contract value in question is below the NSPA Financial Level A (10,000 EUR in 2021).
5. Security: When the security requirements prohibit or restrict the distribution of the RFP data.
6. Commonality of Equipment: When the customer, for training, maintenance or other interoperability reasons, requests that the equipment to be procured must be from the same source as the equipment already in its inventory.⁶

Some standard types of contractual instruments

Depending on the specific terms required, the following standard types of contractual instruments shall be utilised exclusively:

Fixed-Price Contracts: The significance of these contracts is that they provide for the procurement of materiel and/or services at a fixed unit price. This type of contract assets should be utilised unless another type would be more appropriate.

Outline Agreements: Outline agreements set up the specifications, the nature and price of deliverables or the method by which they are to be determined; also, they determine the value and/or quantity of the goods or services.

Outline agreements are executed by purchase orders, issued successively, as needed. Each individual purchase order defines the goods and services that are required, described in the outline agreement, furthermore, determines the necessary quantity.

If, for duly substantiated reasons, it is impossible for a single company to cover all shipments under the most favourable conditions or for a guaranteed reserve, outline agreements for the same shipments may be concluded with several contractors, provided that the agreements expressly specify the conditions under which purchase order may be issued to the various contractors concerned.

Basic Contractual Instruments: The Basic Contractual Instruments (BCIs) set out the negotiated contract term that will apply to future purchases made during the term of the BCI. BCIs can be used when past experience and future plans show that a significant number of separate contracts can be entered into with a contractor during the BCI period and significant recurring negotiation problems arise with a particular contractor. BCIs do not oblige NSPA to place orders or contracts with the contractor.⁷

⁶ OI 4200-01 NSPA Procurement Operating Instructions, NATO Support and Procurement Agency, 18 March 2019.

⁷ OI 4200-01 NSPA Procurement Operating Instructions, NATO Support and Procurement Agency, 18 March 2019.

Establishing commercial contracted capabilities

When establishing a new commercial contracted capability the time required to develop the capability is key. There are different facts and factors that influence this time period and the Agency also works on different practices how to shorten it.

Based on many years of experience, it is proven that the establishment of a new contracted capability, supporting the nations operations, requires approximately 6 months. It is the default practice, when the Agency conducts an international competitive bidding process, calling the capable service providers NATO-wide, from the NSPA Source File. These 6 months starts with the receipt of the requirement and ends with the signed, established contract. (When Single or Sole Source procedure is justified the lead-time is shorter, due to the fact that NSPA needs to conduct the solicitation process with the involvement of only one potential service provider.)

A significant part of the 6 months lead-time is dedicated always to assistance to the customer in developing and, if necessary, amending the Statement of Requirement (SOR). Based on this document, NSPA develops the Statement of Work (SOW), which is the basic document of the RFP process. To shorten the 6 months lead-time, the Agency developed some so-called “SOW+”, in the frame of a kind of contingency planning. Actually, these were pre-planned Statement of Works for the most probable service requirements, which included a kind of template requirement and statements. For example, to support operations, there are SOWs+ for potential base services, food and fuel supply and service requirements, and so on. In case of a firm requirement, these products have been updated and adjusted to the real requirement.

The Basic Contractual Instruments (BCIs) provide a more effective solution in supporting operations. In this case, the NSPA does not conduct a full international competitive bidding cycle but only pre-select the most competent potential service providers. With pre-selecting the potential service providers, a significant part of the solicitation process can be left out later, when the actual task arrives at the Agency. In addition, at this time, NSPA can generate a mini competition between the pre-selected BCI holders. (NSPA provides services through different BCIs, one of them is the Strategic Aeromedical Evacuation Services with two air transport BCI holder companies. This capability provides the services for 5 years based on the valid BCI.)

However, if the Customers need contracted capabilities with (very) short notice time, those capabilities must be ensured in advance through pre-established Assured Access Contracts or dormant contracts. It means that the contracted capabilities have already been established, the necessary assets, supplies, with the associated transport capacity – if required – have been put aside for the customer by the service provider company, but the contract will be activated only if needed. (Recently, assured access contracts are applied by nations that assume tasks in multinational formations with their units in very high readiness, like the Very High Readiness Joint Task Force (VJTF), since neither the NSPA nor any contractors can develop a new contracted capability within a few days to meet the customer’s requirement.)

NSPA hosts 32 Support Partnerships (SP). Nations, using the same weapon systems or are interested in utilising the same services, can establish new SPs to share the

costs, knowledge, experience, also to form and use an asset pool. Two nations suffice to form a new SP and the NSPA support those SPs through the SP Offices manned by the Agency. Each SP is governed by its own Committee (formed by the representatives of the participating nations) and the SPs have their own agreed legal framework. The member nations decide the budget, decide and prioritise the new projects and agree the associated manpower provided by the dedicated SP Office of the NSPA.

Approximately 80 per cent of the requirements arrive to the Agency through SPs. In this case, the customers need to send a simple Tasking Letter and the Statement of Requirement to the given Support Partnership Office to start the process, aiming the development of a new commercial contracted capability. The other basic way of starting the process, is signing a Sales Agreement between the customer nation and the Agency. Since in the latter case the legal questions have not been agreed yet, setting those questions also require some time, extending the period necessary to establish the new contracted capability. Sales Agreement is required if the customer is not a member of the SP which is expected to establish the contracted capability.



Figure 2: The basic lead-time of establishing contracted capabilities for supporting operations

Source: Compiled by the author.

If the customer decides to join already established, ongoing contracted capabilities, the lead-time the NSPA to sign a contract with the contractor, on behalf of the customer, and to start the provision of services is much shorter.

In the area of Support to Operations and Exercises

Today the Agency is organised around the support partnerships and programmes. Recently, the geopolitical situation is changing rapidly. Developments in the Eastern part of Europe, the Middle East and Northern Africa spurred the NATP to change its priorities. Besides

the continuation of the current missions in Afghanistan and Kosovo, new priorities show up on the horizon.

The strategic aim of the NSPA is to provide comprehensive support to the operations, with a special attention to Deterrence and Defence (see later). This requires the Agency to engage early in planning and decision making to respond quickly to emerging requirements. The Contract Integrator capability of the Agency is key to link NSPA to NATO's operational planners. In accordance with that, the Agency has the necessary managerial capability to engage with the leadership in the Allied Command Operations and the nations. NSPA keeps it very important to strengthen and improve existing capabilities, like: fuel, transport and infrastructure. The recent greater emphasis on exercises and interoperability increases demand in this domain. All things considered, the main effort of the Agency is recently to improve the operational responsiveness.

Support to operations area requires a continued attention. The key focus is the need to provide support for Deterrence and Defence related missions and exercises. Expanding the Operational Logistics Support Partnership (OLSP) and the very proactive approach to fuel support for the VJTF is also considered. Other associated NATO operational policies underlined included Contractor Support to Operations and collective contracting including Rapidly Useable Enabling Contracts (RUECs).

The Agency's mission and vision have been updated according to the aforementioned. In particular, 'responsiveness' will be a key factor to ensure that NSPA is able to overcome the upcoming challenges.⁸

New challenges in the supply chain and support to operations

The developments in the Crimea and in East Ukraine in 2014 spurred the NATO to develop and implement new and adequate defence concepts. The new security challenges near the eastern flank of NATO are reflected in the decisions and declarations of the NATO Wales (2014) and Warsaw Summit (2016) when a group of actions and concepts have been articulated to 'deter' any aggression and to provide 'defence' to Europe (Deterrence & Defence or in short: D&D).

The focus shifted from the expeditionary operations to Europe again, new or amended NATO forces, entities, missions were created (like the enhanced NATO Reaction Force (eNRF), NATO Force Integration Units (NFIUs), enhanced Forward Presence (eFP) and so on) with new defence concepts (that is, Graduated Response Plans (GRPs,) creating and applying the VJTF, and so on). The new concepts had a huge impact on the new requirements for contracted capabilities and required a new approach to support to operations from the NSPA, too.

It became clear that in some cases the industry is not responsive enough and cannot satisfy the new requirements, mainly those with very short notice time or the surge requirements. NATO had to re-define the military requirements, re-assess the existing military and industrial capabilities and capacities, including the available and necessary

⁸ Appendix 2 – NSPA Strategic Direction 2018 – 2022 Lines of Development, NSPA Annual Report 2019.

infrastructure, and understand again the operations and practices of the defence industry in Europe.

The multinational cooperation among the NATO member nations, the time factor and the significance of available sources came to the front, and the responsiveness, flexibility and scalability of contracted capabilities got a much higher emphasis.

To fill the forces of the eNRF (and the eFP) annually, the NATO conducts Force Generation conferences when the nations offer their units to NATO through a bidding process. Each year, a willing nation assumes responsibility, as framework nation, for the VJTF, which is an element of the eNRF. Framework nations are volunteered in advance, this way, the units are in a pre-defined rotation that makes possible for the nations to plan the sources of their logistics support ahead. Although the required units are available in the eNRF, their rapid deployment to the east, to secure the eastern flank of NATO, also their sustainment still remained a challenge in some cases (that is, quick deployment of heavy equipment, fuel supply independent of Russian sources, and so on).



The layout of the Central Europe Pipeline System

The Central Europe Pipeline System (CEPS) Programme (NSPA): manages the operation, financing and maintenance of an integrated, cross-border fuel pipeline and storage system in support of NATO’s operational military requirements during peacetime, crisis and conflicts, including expeditionary operations.

Operations run on a 24/7 basis, with the NSPA CEPS Programme Office serving as the liaison between National Organisations and NATO authorities.

Figure 3: The layout of the Central Europe Pipeline System

Source: NSPA/OLSP Basic Overview and Benefits (Agenda Item VIII), Presentation by Mr Dane Tynes, 23rd OLSP Committee Meeting, 20 October 2020.

In the era of the Warsaw Pact, NATO possessed a very reliable logistics supply chain in Western and Central Europe and the responsibilities were also very well outlined. Due to the collapse of the Warsaw Pact, then with the main operations in the Middle East, the security questions in Europe and the previously strictly maintained logistic capabilities and capacities got only a secondary significance. It was the time when the European Ministries of Defence started to outsource some of their tasks and downsize the military

units. Some military capabilities, as well as the civilian capacities, dedicated to military use, were left degrading.

The developments in Ukraine in 2014 found NATO in the above detailed environment making the situation more complex, that is, the remaining reduced capabilities and capacities had to cover double as much geographical area as the territory of the NATO member nations was at the end of the 1980s (the Central Europe Pipeline System was established in 1959 to deliver fuel for military air and ground vehicles in Belgium, France, the Netherlands, Luxembourg and Germany, which country was the eastern flank of NATO until the end of the 1990s).⁹

Potential responses to the challenges through multinational solutions

Due to the new challenges and requirements, the new contracted capabilities have to be flexible and responsive enough to be able to satisfy the military requirements. But how is the D&D sustained currently?

The characteristics are the following:

1. Several Graduated Response Plans established for only one set of NATO forces (which are the units of the eNRF)
2. Large scale strategic movements to and within Europe
3. Annual rotation of forces or elements and rolling sustainment requirements
4. Not clear and firm operational requirements (NATO plans cover limited capabilities)
5. Many multinational formations even below battalion level
6. Limited standing Host Nation Support (HNS) related arrangements (however, there are rolling requirements – like for fuel and food – and high expectations of potential HNS)
7. Higher and higher dependency on commercial support to operations
8. National yearly (one-off) fixed contracts (which expire at the end of the year and a new one has to be established by the beginning of the next year for another nation – that is, for the next VJTF Framework Nation in the rotation plan)

NSPA is the NATO Contract Integrator organisation, which possesses all the capabilities that are necessary for the effective support to nations through contracted capabilities (legal arrangements, common procurement rules, international competitive bidding process, contractual arrangements in one integrated system). NSPA is also capable of receiving/collecting and consolidating requirements so that later it can step up the market with one single requirement representing all the customers. The previously mentioned SPs, within the NSPA, provide perfect platform to the SP member nations for building consensus for multinational commercial solutions. Regarding satisfying the D&D requirements, establishing multinational contracted capabilities is very reasonable since we speak about rolling and recurring supply and service requirements (that is, fuel, food, road/rail

⁹ NSPA official website, Central Europe Pipeline System.

transportation, base services) which are necessary for the different nations' units for their annual rotation (VJTF).

NSPA also had to take into consideration the different characteristics of nations, in other words, nations have different resource allocations, levels of ambition, legal requirements and limitations. Besides the nations' requirements, NSPA had to study the current resources of the market and work out such contracted capabilities which are attractive enough to the market and which covers its interests, as well (that is, multi-year contracted capabilities which are fully utilised).

An already existing SP can provide the platform for the development of a new multinational contracted capability. The member nations of a SP can capitalise of the inherent advantages of the SP (that is, the already existing legal framework and agreed operating mechanism, the shared experience and expertise, and so on).

It is also feasible for the nations under the umbrella of an already existing SP to establish sub-groups for special tasks, so called Project Groups.

The Project Group concept

What does Project Group (PG) mean? In the NSPA we can find examples of functioning PGs under Support Partnerships. Two of them work under the Operational Logistics Support Partnership (OLSP). OLSP is a SP fully dedicated to support to operations. The OLSP has 26 member nations currently and provides support to the member nations through its 4 pillars:

1. Standing legal framework for members to access NSPA services (*no need any sales agreements, a simple Tasking Letter is required in the agreed and OLSP Committee approved form*)
2. Conducts planning with member nations and project development within NSPA (*during the project development, OLSP cooperates with specialised NSPA Program Offices and Divisions – PODs, that is, Fuel or Food Branches, Transportation and Warehousing Division*)
3. Provides National and NATO Exercises training and education support related to commercial solutions for military operations
4. Facilitates, innovates and develops multinational commercial solutions¹⁰

The OLSP Support Partnership Committee makes OLSP possible to establish PGs. A PG is formed by those OLSP member nations that use the given service and the PG gives the governance of the service. The basic frame of the service is the OLSP legal framework. The PG makes decisions on the operation of the subject service, decides the rules of the operations, the budget and the NSPA personnel associated to support the management and execution of the services. The first PG was established in 2019 for the Global Food Services. The success of the Global Food Services has already been proven, providing food

¹⁰ NSPA/OLSP Basic Overview and Benefits (Agenda Item VIII), Presentation by Mr Dane Tynes, 23rd OLSP Committee Meeting, 20 October 2020.

supply and services currently to the Netherlands, Italy and the United States in Europe and in the Middle East.

Some of the OLSP member nations have already realised the advantages of the PGs and articulated clearly in the SP Committee Meetings or individually to the SP Office that more and more multinational framework contracts are needed under SPs providing support to operations. If so, OLSP found it feasible to offer governance and management option under the existing, well-functioning and responsive partnership. Furthermore, capitalising on the experiences of the already existing Global Food Services Project Group would make it possible to re-award the success of that PG, saving costs, time and additional efforts for the nations.

Responsibilities of the member nations in a PG: The PG steers the given service. The member nations fund the service and participate in the PG meetings, deciding on future activities and objectives. The PG assigns specific tasks to be performed within the context of the given service and the objectives of the specific PG. Furthermore, the PG forecasts and approves the program of work for the service, inclusive of future projects and potential support requirements. The program of work provides transparency for forthcoming requirements and helps to prioritise the use of services and the NSPA workforce. Each member nation of the PG provides a national official representative.

Responsibilities of the NSPA SP Office: The NSPA SP Office is the administrative entity that provides oversight and coordination for all project activities. The SP Office coordinates the PG meetings and reports the PG member nations.

In the NSPA comprehensive concept to sustain the D&D related requirements of the nations the most properly, the Project Group concept is only one element.

Beyond the challenges in supporting the D&D related requirements, described in section *New challenges in the supply chain and support to operations*, NSPA had to consider all the factors which may cause a potential risk to the establishment and provision of seamless contracted services to the nations. These factors can be:

1. too high cost of services
2. too long lead-time to start the services
3. lack of capable service providers or dominant non-NATO country (that is Russian) ownership over sources and facilities (that is, fuel sources and facilities in Eastern Europe)
4. reluctance of the market to answer the nations' call, because of non-doable requirements or economy of scale
5. non-compliance or late delivery by the service provider or interruption of services
6. too rigid frames of existing contracted capabilities which reduces the opportunity to be used by additional nations, the contract to be scalable

NSPA had to address those risks, too.

Creative Defence Contracting

Due to the new D&D concepts, using military units provided by rotating framework nations, the nations stepped up with more and more requirements for support to operations. To overcome the factors, mentioned in section *The Project Group concept*, which may pose risks to the establishment of contracted capabilities, and to find the contracted solutions, which are equally favourable to both the nations and the market, NSPA had to think of contracting procedures and principles through a new and creative lens. NSPA realised that the defence concept related timelines have to drive the characteristics of the contracted capabilities. Furthermore, to be able to satisfy different national requirements, NSPA had to consider the different national resource allocations, the national legal requirements and limitations, as well as the different national levels of ambition. Also, the new contracted capabilities should satisfy the short noticed and recurring requirements thereby avoiding repetitive commercial procurement procedures every time when a new operational support requirement arrives. All of this entailed the creation of new contracting approach and principles.

The new support to operations requirements can be satisfied through standing, scalable, adaptable and flexible contracted capabilities, which are available to all nations and can provide contracted services to the rotations of different military units, as well. The services, collected in packages or modules, make possible the national or multinational requirements to be served from a 'menu' that takes into account the special national needs. Based on the aforementioned, the Creative Defence Contracting Principles that have to be considered and applied are:

1. contracted capability with modularity and scalability
2. long term contracted capability, 3 years or more (usable by eNRE, VJTE, HNS, eFP)
3. indefinite delivery and quantity element
4. adaptable and flexible
5. economies of scale
6. responsiveness against readiness requirements
7. satisfying recurring and rolling requirements
8. applying the multinational Project Group concept
9. applying payback mechanism¹¹

Example of the new type of multinational contracted capability

The OLSP Global Food Services

The Global Food Services (GFS) is a NSPA standing and global capability with scalable and turnkey food services for nations deployed abroad or on exercises. The services are under the OLSP umbrella and governed by the Global Food Services Project Group (GFS PG). The establishment of the contracted capability is sponsored by the Netherlands, which is the only PG member currently. The capability is accessible to all nations. GFS comprises of three capability

¹¹ György Gulyás, Synopsis of the Final Report for the Multinational Rail Transport Services Feasibility Study, Agenda Item XII, Presentation, 23rd OLSP Committee Meeting, 20 October 2020.

packages or modules: Food Supply (only supplies without any services), Human Resources (performing catering, storing, cooking or other food related services) and Catering Operations. The capabilities are scalable in order to meet the requirements of all nations. It is a global capability with the main focus areas in Europe, Africa and the Middle East. The services can be delivered within 90 days of the received requirement.

The GFS contract was awarded on 1 March 2019. The contract mechanism is a hybrid solution, which is a Basic Contractual Instrument (BCI) where outline agreements have been awarded to multiple service providers. A total of four commercial companies hold outline agreements across the three GFS capability packages. The contract call-offs are executed in accordance with the customer requirements, so nations use only the package which fits best to the given military task or mission to be supported. Due to the contract volume, the scope and scale, as well as to maintain competitive advantage, each call-off is based on dual source as a minimum.



Within the Catering Operations food, bottled water and catering services can be found, including an option for a stand-by capability (or a dormant element of the package) supporting the units in very high readiness.

Figure 4: The Capability Packages of the Global Food Services

Source: John Goering, OLSP Global Food Services, Agenda Item XIII, Presentation, 23rd OLSP Committee Meeting, 20 October 2020.

This call-off process makes possible for the NSPA to choose the best offer from the service providers for each requirement, maintaining competitiveness, as well as permanent optional sources.

NSPA/OLSP encourages the nations to join the GFS PG. This way they can decide on the future projects of the services and can have an influence in governing the services. Although the costs of maintaining the GFS (that is, the salary of the OLSP Office associates dedicated to the support of the GFS) is paid by the GFS PG member nation(s), OLSP worked out a payback mechanism: the non-PG member nations have to pay a fee, furthermore, non-OLSP member nations pay usage fee and surcharge when they use the services (GFS fees and surcharges levied in accordance with NSPO Directive No. 3999 and approved during the 19th OLSP Committee Meeting). The fees and surcharges offset the administrative (GFS related overheads, like salaries) and operational costs (actual cost of a service) of the PG member(s).¹²

¹² John Goering, OLSP Global Food Services, Agenda Item XIII, Presentation, 23rd OLSP Committee Meeting, 20 October 2020.

Summary

The above new type contracted capability brought a lot of benefits to the customer nations. Naturally, there were (and exist) many other multinational contracted capabilities offered by different Program Offices or Divisions of the NSPA (that is, the Global Access Services, which provides worldwide provision of plane refuelling services) but the GFS was the first one which was established with such a comprehensive approach addressing the new type of requirements. These types of capabilities are able to support requirements with a 'normal' lead-time but also very short-noticed ones for units in very high readiness. The services are available in peacetime, crisis and war worldwide.

Their basic benefits are among others:

1. Standing capability with established governance (Project Group) and Terms of Reference under a standing Support Partnership – no need for a Sales Agreement, no need to develop a specific SOW when sending the requirement to the NSPA
2. The standing capabilities have been established with high value for future scalability, services are open to all nations (including non-Project Group member and non-Support Partnership member countries)
3. The sponsoring nation funds the cost of manpower to maintain the capability within the Project Group – but offset through fees and surcharges
4. The contracted capability packages/modules are in place with outline agreement holders – no need for a protracted competitive bidding process only a 'mini competition' among the outline agreement holders, when an exact task arrives at the NSPA for the services
5. Achieved reduced lead-time from tasking to contracting – from 6 months to 90 days
6. The capability packages/modules function like a 'menu' – nations can chose the proper one which fits the best to their military mission, budget and other national characteristics
7. The services can properly satisfy the annual rotation of force elements (that is, VJTF framework nations) and also the rolling sustainment requirements

With this type of multinational contracted solution, applying the PG concept, the nations are heavily involved in the decision making process, deciding what future projects should be launched next, what budget shell be used, always keeping in mind their national interests. NSPA can re-award the success of this contracted capability with establishing new ones, depending on the nations' interests, to cover the most demanded services that can come into question in case of operations. The establishment of the Global Fuel Services contracted capability is nearing its end (sponsor – and PG member nation – is the Netherlands) and the development of the Global Base Services capability starts recently (sponsor is the United States) applying the PG concept in both cases.

The NSPA developed a new generation of the multinational contracted solutions with new contracting technics and new governing concept. Now the nations should decide what additional capabilities should be established taking into account their national interests and assessing where their requirements can fit in the new capabilities. Or, in another way, how those current and future capabilities could best serve their national or multinational

military missions. In a direct or indirect way, the new contracted capabilities serve effectively the collective NATO defence efforts, as well.

References

- AJP-4(B) Allied Joint Logistics Doctrine. Online: https://assets.publishing.services.gov.uk/government/uploads/attachment_data/file/907825/doctrine_nato_logistics_ajp_4.pdf
- Appendix 2 – NSPA Strategic Direction 2018 – 2022 Lines of Development, NSPA Annual Report 2019. Online: www.nspa.nato.int/resources/site1/General/publications/NSPA_Annual_Report_2019_e.pdf
- Balla, Tibor, *Civil és katonai javak a szerződött logisztikai szolgáltatások tükrében* [Civilian and military goods in the light of the contracted logistical services]. PhD dissertation, Budapest: Miklós Zrínyi National Defence University, 2004. Online: www.uni-nke.hu/document/uni-nke-hu/balla_tibor.pdf
- Goering, John, OLSP Global Food Services, Agenda Item XIII, Presentation, 23rd OLSP Committee Meeting, 20 October 2020. Online: <https://eportal.nspa.nato.int/public/eportal.aspx>
- Gulyás, György, Synopsis of the Final Report for the Multinational Rail Transport Services Feasibility Study, Agenda Item XII, Presentation, 23rd OLSP Committee Meeting, 20 October 2020. Online: <https://eportal.nspa.nato.int/public/eportal.aspx>
- Jávör, Endre, *A befogadó ország logisztikai támogató tevékenysége többnemzetiségű békefenntartó hadműveletben, különös tekintettel a magánjogi szerződések alapján történt végrehajtásra* [Logistical support activities of the host nation in a multinational peacekeeping operation, with special regard to the implementation under private law contracts]. PhD dissertation, Budapest: Miklós Zrínyi National Defence University, 2002. Online: <http://ludita.uni.nke.hu/repozitorium/bitstream/handle/11410/8961/Tartalomjegyz%C3%A9k%21?sequence=1&isAllowed=y>
- NSPA official website, www.nspa.nato.int/about/history
- NSPA official website, Central Europe Pipeline System, www.nspa.nato.int/about/ceps
- NSPA/OLSP Basic Overview and Benefits (Agenda Item VIII), Presentation by Mr Dane Tynes, 23rd OLSP Committee Meeting, 20 October 2020. Online: <https://eportal.nspa.nato.int/public/eportal.aspx>
- OI 4200-01 NSPA Procurement Operating Instructions, NATO Support and Procurement Agency, 18 March 2019. Online www.nspa.nato.int/resources/site1/General/business/procurement/General%20info/OI-4200-01-EN.pdf
- OI 4200-01 NSPA Procurement Operating Instructions, NATO Support and Procurement Agency, 18 March 2019. Online: www.nspa.nato.int/resources/site1/General/business/procurement/General%20info/OI-4200-01-EN.pdf

Can Boko Haram Constitute a Threat to European Security?

Tibor BABOS¹ – Gábor SINKÓ²

Imbalance, poverty, dictatorship's expansionary ambition and the relevant cultural background serve as fertile ground to expand terrorism.³

Tibor Babos

In this study, the authors seek to address the question whether Boko Haram can constitute a threat to European security. To answer this question, one must analyse recent Nigerian migration patterns to Italy, actual reports, peer-reviewed academic works, a wide variety of regional journals and media articles. By evaluating all available research sources, it can be concluded that the answer is not as clear-cut as one might think at first glance. On the one hand, we could argue that a terrorist group like Boko Haram cannot constitute a serious European security threat, since the majority of Nigerians arriving in Europe seems to have decided to flee their country of origin due to economic, social and security reasons, therefore, these migrants have nothing to do with terrorism. On the other hand, we could also argue that Boko Haram can pose a threat to European security, by taking advantage of migration flows and inserting its own soldiers, thus creating terrorist cells within them. We have found plenty of evidences related to the terrorist organisation's increased use of women as soft targets and the potential re-radicalisation of traumatised children in Europe. Since its alignment with ISIL in 2015, there has been growing concern that Boko Haram could follow suit with focusing its efforts on refugees, infiltrating migration flows and thereby creating a significant security risk to Europe. However, in recent years the number of Nigerian migrants arriving in Europe has been decreasing, which could be justified by tighter links between African and European governments and by stronger European control. If this continuous cooperation and tight internal European border security and police procedures are to remain, there is less chance for Boko Haram to constitute a threat to European security.

Keywords: Boko Haram, European security, Nigeria, migration, infiltration

¹ Associate Professor, Donát Bánki Faculty of Mechanical and Safety Engineering, Director of Óbuda University Center for Safety Sciences, Honorary Professor of Óbuda University; e-mail: babos@uni-obuda.hu

² Doctoral student, Óbuda University Doctoral School of Security Sciences; e-mail: sinko.gabor@stud.uni-obuda.hu

³ T Babos, *The Five Central Pillars of European Security* (Brussels: NATO Public Diplomacy Division, Budapest: Strategic and Defense Research Center, Oberammergau: NATO School, Budapest: Charta press, 2007).

Introduction

9/11 not only shook the world but also caused significant change in security policy perceptions. What previously were only potential risk factors are now everyday threats. Following the terrorist attacks, the quantitative indicators and distribution of the world's security factors did not change; however, the quality and nature did. Looking at targets, it is evident that military sites are only secondary and attacks against civilians, besides military targets, directly and significantly revised the previous rules of warfare. The vulnerability of developed countries did not diminish; however, national and state defensive systems required fundamental revisions.⁴

We can be certain that fanatics with relative power status are prepared and able to sacrifice people – both followers and victims – for their cause. Considering that the majority of terror planners send misguided or threatened women and young men to commit suicide attacks, taking steps against them is extremely difficult. The after-effects of major attacks mean economic and societal changes on the national level. Anti-terrorism campaigns also demand increased expenditures and tax resources worldwide, which bring about numerous restrictions on mass transport and strategically significant facilities.⁵

One of the most dominant matters of recent European history is the large inflow of migrants and refugees arriving in the European Union (EU) from all across the world. According to a 2018 Eurostat spreadsheet, the number of people applying for asylum in the EU quadrupled between 2013 and 2015.⁶ Moreover, from the latter year migration has featured more prominently in public discussions and thereby entered the collective consciousness of European citizens and has remained to be one of the most worrisome issues in the following years.⁷

There has been much emphasis on the influx of refugees coming to the EU from the Middle East, especially from Syria due to the civil war that is still raging in the country. Nevertheless, Africa also deserves special attention, since nearly a threefold increase could be witnessed in the number of asylum applicants comparing data in 2008 and 2018.⁸ Furthermore, while there were fewer Iraqi and Syrian refugees arriving in the EU after the peak of the European migrant crisis in 2015, the inflow of African asylum seekers continued to show a steady increase. Considering the number of asylum applications between 2008 and 2017, refugees from Africa regarded Italy, France and Germany as the most favourable target countries. Additionally, the European population of migrants from Sub-Saharan Africa has grown by almost a million between 2010 and 2017.⁹

⁴ Ibid.

⁵ Ibid.

⁶ Eurostat, 'Asylum and new asylum applicants: monthly data', 2018.

⁷ European Commission, Standard Eurobarometer 89 – Wave EB89.1. Kantar Public Brussels on behalf of TNS opinion & social, Survey requested and co-ordinated by the European Commission, Directorate-General for Communication, Fieldwork, March 2018.

⁸ H Weber, 'Can Violent Conflicts Explain the Recent Increase in the Flow of Asylum Seekers From Africa Into Europe?', *Journal of Immigrant & Refugee Studies* 17, no 4 (2019), 405–424.

⁹ Pew Research Center, 'At Least a Million Sub-Saharan Africans Moved to Europe Since 2010', 22 March 2018.

In this article, the authors seek to address the question whether one of the most lethal terrorist organisations, *Boko Haram* constitutes a threat to European security. According to previous studies, terrorism could be considered one of the most perilous phenomena from the perspective of global security and peace.¹⁰ It seems evident that in the 21st century, which is increasingly characterised by changing geopolitics and globalisation, exchanges and flows have largely been facilitated. Besides being a force for good, they have been exploited by terrorist groups for network-developmental and recruitment purposes.¹¹

Today the Nigerian Jama'atu Ahlis-Sunna Lidda'Awati Wal-Jihad (People Committed to the Prophet's Teachings for Propagation and Jihad) or as more commonly known, *Boko Haram* continues to pose a major threat both locally and globally, especially after pledging allegiance to the Islamic State of Iraq and the Levant (ISIL) in 2015.¹² While the spillover of its military activities to neighbouring countries has had an effect on regional security, the authors intend to scrutinise if there could be a potential link between *Boko Haram* and European security by analysing reports, peer-reviewed academic works, journals and recent Nigerian migration patterns to the most important target country by the Mediterranean Sea, Italy. Additionally, despite them being fragmentary or politicised, media articles have been utilised with the intention of painting a clearer image.

The thesis of the study is that not only does *Boko Haram* constitute a threat to regional security in Nigeria and its neighbouring countries but also to Europe. In order to verify this claim, firstly the authors examine Nigerian migration patterns with their potential push and pull factors, perform a background analysis of *Boko Haram* and review the major historical events in the development of the terrorist organisation. The study then analyses and evaluates the European aspects of the group and finally draws conclusions and makes recommendations with regard to *Boko Haram*.

Background

Since the beginning of the European migrant crisis, high numbers of refugees and migrants have started arriving in the EU. Over the years, Italy could be regarded as the most popular destination country for African nationals traveling through the Mediterranean Sea.¹³ Most of the people who arrived in Italy in the period of 2014–2015 were of Syrian, Nigerian, Sudanese, Gambian, Ethiopian, Somali and Bangladeshi origin.¹⁴ Table 1 illustrates the number of African migrants coming to Italy by sea between 2015 and 2018, coupled with

¹⁰ C Flint, *Introduction to Geopolitics* (New York: Routledge 2011); A R Moten, 'Understanding Terrorism: Contested Concept, Conflicting Perspectives and Shattering Consequences', *Intellectual Discourse* 18, no 1 (2010), 35–63; L Pettiford and D Harding, *Terrorism: The New World War* (London: Arcturus Publishing Limited, 2003).


¹¹ C Isike and E Isike, 'Migration and the geopolitics of Boko Haram terrorism in Nigeria', *Strategic Review for Southern Africa* 40, no 2 (2018), 34–51.

¹² I Inyang, 'Boko Haram is broke – UN Envoy', *Daily Post*, 08 February 2017.

¹³ European Commission, Standard Eurobarometer 89; J Besenyő, 'Fences and Border Protection: The Question of Establishing Technical Barriers in Europe', *AARMS* 16, no 1 (2017), 77–87.

¹⁴ IOM, 'Migration Trends Across the Mediterranean: Connecting the Dots', *Altai Consulting for IOM MENA Regional Office*, June 2015.

their countries of origin. As it can be seen, besides Eritrea, Nigeria was responsible for the largest inflow of irregular refugees and migrants to Italy with its nearly 78,000 people in the period of 2015–2017. By 2018, the number of Nigerians arriving in Italy has dropped significantly, since only 1,250 people were registered at the country's shore.¹⁵ In the last two years, however, Nigeria was not even included in the list of the ten most common nationalities of arrivals in Italy.¹⁶

 Mediterranean Developments Tables 4				
ARRIVALS BY SEA TO ITALY - NATIONALITIES				
MAIN COUNTRIES OF ORIGIN				
2015-2018				
(source: Italian Ministry of Interior)				
Main Countries of Origin	2015	2016	2017	2018
Tunisia	880	1,207	6,151	5,002
Eritrea	39,162	20,718	7,052	3,32
Sudan	8,932	9,327	6,221	1,619
Nigeria	22,237	37,551	18,158	1,25
Côte d'Ivoire	3,772	12,396	9,507	1,05
Mali	5,826	10,01	7,118	876
Guinea	2,801	13,342	9,701	810

Update 11/12/18

Table 1: Arrivals of African migrants by sea to Italy between 2015 and 2018

Source: IOM UN Migration, 'Mediterranean Migrant Arrivals'.

As a consequence of the increase in the number of Nigerian illegal migrants and refugees between 2015 and 2018, tougher migration policies have been adopted by European leaders with the intent of regulating and controlling migration flows to the continent. In search of higher standard of living, Nigerians had to come up with an alternative path for getting into Europe, which was ultimately found in the CentralMediterranean route.¹⁷ It has been reported to be one of the most dominant crossovers for African nationals, particularly those emigrating from either the north or the west of the continent.¹⁸ The spike in the arrivals of Nigerian migrants in Italy in 2016 might be explained by *Boko Haram* pledging allegiance to ISILthe previous year. This view is supported bythe results of a 2015 Global Attitudes Survey, according to which 66 per centof Nigerians had an unfavourable opinion

¹⁵ IOM UN Migration, 'Mediterranean Migrant Arrivals Reach 110,833 in 2018; Deaths Reach 2,160', 12 November 2018.

¹⁶ UNHCR, 'Italy Sea Arrivals Dashboard', December 2019; UNHRC, 'Italy Sea Arrivals Dashboard', October 2020.

¹⁷ K Hooper, 'European Leaders Pursue Migration Deals with North African Countries, Sparking Concerns about Human Costs', *Migration Policy Institute*, 17 December 2017.

¹⁸ IOM, 'World Migration Report 2018'; DTM, 'Libya's Migrant Report', *Flow Monitoring*, Round 17, January–February 2018.

of the Islamic militant group in Iraq and Syria.¹⁹ Nevertheless, while *Boko Haram* is mostly active in the northeast, the majority of Nigerian refugees coming to the EU appear to have originated from Benin City, which is situated in the south of the country.²⁰

When studying the causes of Nigerian migration, it is elementary to scrutinise its potential push and pull factors. These can either be applicable for individuals or groups and are simultaneously present with some of them being more or less significant depending on context.²¹ There are elements capable of pushing refugees away from their country of origin and there are factors that can pull them in their destination countries. Political instability, human rights abuses and government repression, for instance, are thought to have largely contributed to the increase in the inflow of Nigerian migrants to Europe.²² Corruption is another often-cited element that may have led to the inability of the Nigerian Government to provide basic services to its citizens, especially in the northern part of the country, where the influence of *Boko Haram* is the strongest.²³

Economic factors, such as the lack of job opportunities and poverty feature as major causes of Nigerian migration, as well. When poverty headcount rates in some of the northern (Yobe 72.34 per cent, Gombe 62.31 per cent, Adamawa 75.41 per cent) and southern states (Lagos 4.5 per cent, Delta 6 per cent, Edo 12 per cent) are compared, huge differences can be seen.²⁴ Illiteracy constitutes another problem with the amount of illiterate youth being at 83 per cent in *Boko Haram*-ridden Borno state.²⁵ Besides, one of the most important responsibilities of a government is the protection of its citizens' lives. If it fails to do so then a reasonable response from the population could be migration to another country that is able to provide security. In this sense, terrorism in the form of religious and political insurgencies in Nigeria can also be considered a push factor.²⁶

¹⁹ J Poushter, 'In nations with significant Muslim populations, much disdain for ISIS', *Pew Research Center*, 17 November 2015.

²⁰ S O'Grady, 'Nigerian Migrants Get a Welcome Home. Jobs Are Another Story', *New York Times*, 08 January 2018; BBC, 'A Nigerian's nightmare failed bid to migrate to Europe', 28 April 2017; J Agbakwuru, 'FG inaugurates Migration Centre in Edo', *The Vanguard Nigeria*, 07 March 2018.

²¹ A Loada and P Romaniuk, 'Preventing Violent Extremism in Burkina Faso: Toward National Resilience Amid Regional Insecurity', *Global Center on Cooperative Security*, June 2014.

²² M O Okeyim, *The State and Migration of Nigerians into the European Union to Live in Spain* (Doctoral thesis, University of Alicante, 2012); A Botha, 'Radicalisation in Kenya: Recruitment to al-Shabaab and the Mombasa Republican Council', *ISS Paper 265*, September 2014.

²³ R C Cachalia, U Salifu and I Ndung'u, 'The dynamics of youth radicalisation in Africa: Reviewing the current evidence', *ISS Paper 296*, August 2016.

²⁴ NBS, '2019 Poverty and Inequality in Nigeria: Executive Summary', *National Bureau of Statistics*, 2019.

²⁵ D E Agbiboa, 'The Nigerian burden: religious identity, conflict and the current terrorism of Boko Haram', *Conflict, Security & Development* 13, no 1 (2013), 1–29.

²⁶ B Barungi, O Odhiambo and R Asogwa, *African Economic Outlook 2017: Nigeria* (African Development Bank, OECD Development Centre, UNDP, 2017).

A Brief History of Boko Haram

According to the Global Terrorism Index, *Boko Haram* could be regarded as the deadliest terrorist organisation in the world in 2015, and lost only one position a year later.²⁷ Since the beginning of the insurgency, tens of thousands of people have been killed and a large number of Nigerians have been forced to leave the country, migrating to the neighbouring territories of Chad, Niger and Cameroon.²⁸ The intensification of brutality against the government started after the execution of the group's former leader, Mohammed Yusuf in 2009. However, at that time there was no widespread fear experienced by civilians, since the Islamist sect's primary target was Nigerian security forces. As a reaction to the insurgency, the government abused power and legitimised the excessive use of force against the fighters of *Boko Haram*, which has arguably paved the way for radicalisation. The blanket application of high degree of violence by the Nigerian police may have deprived the terrorist group of the possibility for engaging with politics purposefully.²⁹

The period between 2010 and 2013 was characterised by an increasing number of civilian casualties, although the jihadist terrorist organisation attempted to issue warnings with the intent of minimising death toll in territories where attacks were planned. Furthermore, *Boko Haram* seemed to have enjoyed popular support during that time, since the terrorist group was likely to be viewed as an alternative to what the population, especially in the northeastern part of the country, perceived as an incompetent government. A woman from Borno stated that 'the community perception about [*Boko Haram*] was that [...] they are a new sect that is coming in peace because at the beginning they showed love and concern, and [they] provided things to needy people of the community'.³⁰ On the contrary, there was growing antipathy to Nigerian security forces, which was caused by their brutality in retaliation.³¹

Following the death of the group's founder, one of his deputies, Abubakar Shekau became the leader of *Boko Haram*. Over time, the name of the terrorist organisation was intertwined with the escalation of violence in Nigeria and its neighbouring countries and the significant expansion of 'legitimate' targets based on the rather narrow, Salafist interpretation of the Qur'an. The former official spokesperson of the Islamist sect, Abu Qaqa emphasised that 'even if you are a Muslim and do not abide by sharia, we will kill you'.³² Therefore, Muslims who did not comply with the group's strict version of

²⁷ GTI, *Measuring and Understanding the Impact of Terrorism* (Institute for Economics and Peace, 2015); GTI, *Measuring and Understanding the Impact of Terrorism* (Institute for Economics and Peace, 2016).

²⁸ C Gaffey, 'Why are over 1 million displaced persons in Nigeria too scared to go home?', *Newsweek*, 12 October 2017.

²⁹ C Felter, 'Nigeria's Battle with Boko Haram', *Council on Foreign Relations*, 08 August 2018.

³⁰ Mercy Corps, 'Motivations and Empty Promises: Voices of Former Boko Haram Combatants and Nigerian Youth', April 2016, 14.

³¹ S Ladbury et al., 'Jihadi Groups and State-Building: The Case of Boko Haram in Nigeria', *Stability: International Journal of Security & Development* 5, no 1 (2016), 1–19.

³² M Mark, 'Boko Haram vows to fight until Nigeria establishes sharia law', *The Guardian*, 27 January 2012.

Islam were growingly targeted through *takfir*, the practice of stating that a Muslim can be regarded as a non-believer.³³

Since 2016, *Boko Haram* has been comprised of two factions with both of them allegedly affiliated with ISIL. In 2015, Abu Musab al-Barnawi was named as the new leader of the terrorist group.³⁴ Despite the fact that ISIL had issued a statement about the replacement of the former leader, Shekau continued operations and claimed he was still in charge of *Boko Haram*, accusing al-Barnawi of attempting a coup against him.³⁵ Following the splintering of the terrorist organisation, Shekau's faction could rather be characterised by the preference of indiscriminate attacks on internally-displaced people (IDPs), while al-Barnawi's faction seemed to favour more direct engagement with Nigerian security forces.³⁶ While *Boko Haram* cannot be considered a unified group, the movement remains lethal and active; this is illustrated by a sharp rise in deaths in April 2020.³⁷

Due to the fact that a sevenfold increase could be experienced in the number of civilian casualties between May and August 2017, the Nigerian military launched a comprehensive operation under the codename 'Deep Punch' in the northeast of the country. Their purpose was to decimate and drive out the remnants of *Boko Haram* from Sambisa Forest. The military offensive proved to be rather successful, because the terrorist organisation was distanced from urban areas and also lost territories.³⁸ However, there is growing fear that if *Boko Haram* is not defeated, Europe must ready itself for a new wave of migration with terrorists arriving in the continent. Fatima Akilu, a NHS psychologist and leader of the country's de-radicalisation program argued that 'as *Boko Haram* gets squeezed in Nigeria by the military, what is the next stage? Embed themselves in other countries far from their homeland? That could be the plan'.³⁹

Infiltration to Europe?

After the success of 'Deep Punch', *Boko Haram* retreated to more remote locations and increased the usage of soft targets, such as women, kids and refugees for committing suicide attacks. According to the Institute for Security Studies, a growing tendency can be witnessed in the group's assaults with four attacks perpetrated in 2015, ten a year later and fifteen until September 2017.⁴⁰ As it can be seen in Figure 1, women, especially in Sub-Saharan Africa, have been responsible for a great number of suicide bombings recently,

³³ O S Mahmood, 'More than propaganda: A review of Boko Haram's public messages', *ISS, West Africa Report* 20, March 2017.

³⁴ BBC, 'Boko Haram in Nigeria: Abu Musab al-Barnawi named as new leader', 03 August 2016.

³⁵ The Sun, 'Boko Haram allegedly split over leadership', 17 July 2018.

³⁶ O S Mahmood, 'Boko Haram in 2016: A highly adaptable foe', *ISS Today*, 07 February 2017.

³⁷ J Campbell, 'Nigeria Security Tracker', *Council on Foreign Relations*, 12 October 2020.

³⁸ Amnesty International, 'Lake Chad region: Boko Haram's renewed campaign sparks sharp rise in civilian deaths', 05 September 2017; J Akubo, 'Boko Haram: Army unveils operation 'deep punch' for final push', *The Guardian Nigeria*, 09 July 2017.

³⁹ J W Simons, 'Boko Haram jihadists 'set to infiltrate Europe through Libya' as Nigeria's humanitarian crisis threatens NEW WAVE of illegal migration', *MailOnline*, 13 February 2018.

⁴⁰ A-N Mbiyozo, 'How Boko Haram specifically targets displaced people', *ISS Policy Brief*, 06 December 2017.

possibly due to their ability to get close to their targets without arousing much suspicion and not being as thoroughly searched as men.⁴¹ Besides, female suicide bombers get more screen time, which is a possibility for terrorist organisations to disseminate ideology and may also shame males into recruitment.⁴²

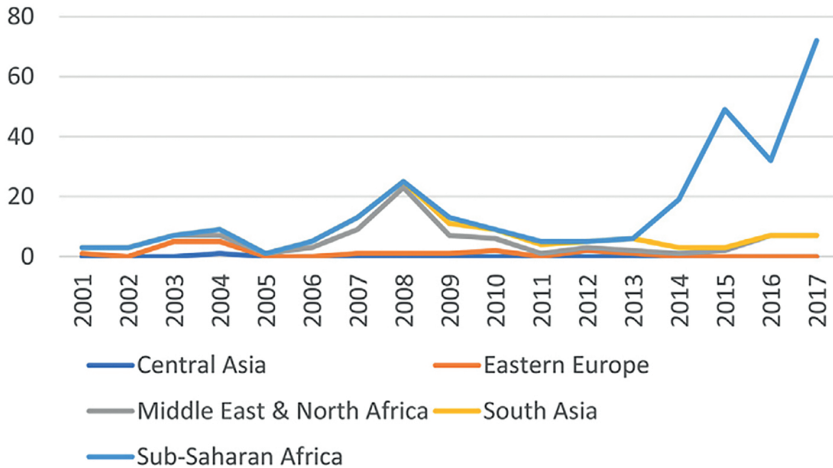


Figure 1: Female suicide bomb attacks by region 2001–2017⁴³

Currently there are approximately 294,000 Nigerian refugees, over 2 million IDPs in the country and more than 684,000 IDPs in neighbouring territories, including Cameroon, Chad and Niger.⁴⁴ There is an increasing number of youths in Nigeria who started dreaming of finding work in Europe, since ‘sending Euros home – a stronger currency – will make a big difference to their families’.⁴⁵ Economic migration stems from the lack of job opportunities and poverty in Nigeria with the latter being exploited by *Boko Haram* itself. For instance, pupils of Qur’anic institutions, the *almajiri* are sent out to the streets in the northern part of the country to beg for two and a half hours every day in exchange for their education provided by these schools. This, in turn, may pave the way for radicalisation as kids can be approached by *Boko Haram* members offering them a chance for a better life.⁴⁶

⁴¹ M Bloom, ‘Female suicide bombers: a global trend’, *Daedalus* 136, no 1 (2007), 94–102; M Bloom, ‘Bombshells: Women and Terror’, *Gender Issues* 28, no 1 (2011), 1–21; A Dalton and V Asal, ‘Is It Ideology or Desperation: Why Do Organizations Deploy Women in Violent Terrorist Attacks?’, *Studies in Conflict & Terrorism* 34, no 10 (2011), 802–819.

⁴² M Bloom, *Dying to Kill: The Allure of Suicide Terror* (New York: Columbia University Press, 2005); J Davis, *Women in Modern Terrorism: From Liberation Wars to Global Jihad and the Islamic State* (Lanham: Rowman & Littlefield Publishers, 2017).

⁴³ J Galehan, ‘Instruments of violence: Female suicide bombers of Boko Haram’, *International Journal of Law, Crime and Justice* 58 (2019), 113–123.

⁴⁴ UNHCR, ‘Nigeria emergency’, 2020.

⁴⁵ J Burpee, ‘A Deadly Journey: Desert, Sea, Detention... On the Road to Europe’, *IOM*, September 2017.

⁴⁶ I Aghedo and S J Eke, ‘From Alms to Arms: The Almajiri Phenomenon and Internal Security in Northern Nigeria’, *The Korean Journal of Policy Studies* 28, no 3 (2013), 97–123.

Religion has also been used as a recruitment tool in the Nigerian context as it can be regarded as a ‘vehicle to voice [emotional or moral] outrage and provides a space for common identity that youth seek’.⁴⁷ Additionally, there seems to be a connection between psychological trauma or spiritual crisis experienced by the youth and their recruitment to extremist organisations,⁴⁸ which is attested by the story of Hassan, whose whole family was coerced into joining the ranks of *Boko Haram* and went through ideological indoctrination. He later stated that ‘[he had seen] a lot of people getting killed but [he had never been] selected for an operation. [He had] wanted to be selected. It would [have given him] pride, [he would have] loved it’.⁴⁹

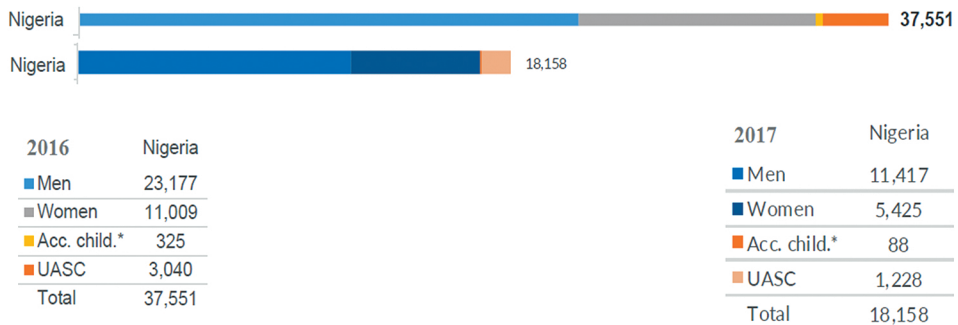


Figure 2: Nigerians of sea arrivals to Italy by gender in 2016 and 2017

Source: Compiled by the author.

As illustrated in the figure above, the majority of Nigerians arriving in Italy by sea in 2016 and 2017⁵⁰ was comprised of men. The number of women was approximately half as many as their counterparts, with children accounting for less than 10 per cent of European migration flows. At first glance, this data does not seem to be staggering as 181,436 and 119,369 migrants and refugees arrived at the shores of Italy in the given years respectively and Nigerians – although one of the most represented nationalities – was only a part of the influx of individuals coming to Italy and thereby Europe by sea.⁵¹

Men are commonly utilised for traditional warfare; however, it seems that it is worth studying the potential reasons why women are increasingly used for suicide bombings by *Boko Haram*. Considering long-prevailing inequalities in terms of education, employment, gender development, literacy and reproductive health, countries in Sub-Saharan Africa are positioned at the bottom of the table.⁵² As a consequence, the life of a woman probably does not carry much value in the eyes of *Boko Haram*, particularly those who do not show any

⁴⁷ Cachalia et al., ‘The dynamics of youth radicalisation’, 18.

⁴⁸ M Ranstorp, ‘Terrorism in the Name of Religion’, *Journal of International Affairs* 50, no 1 (1996), 41–62.

⁴⁹ Simons, ‘Boko Haram jihadists’.

⁵⁰ Gender-based data from UNHCR could only be extracted for these specific years.

⁵¹ UNHCR, ‘Nigeria emergency’, 2020.

⁵² Human Development Report, *The next frontier: Human development and the Anthropocene* (New York: UNDP, 2020).

signs of adherence to the strict, Salafist interpretation of Islam. Females are therefore seen as inexpensive commodities, serving the interests of the terrorist organisation, since the benefits *Boko Haram* is likely to reap after the either successful or unsuccessful outcome of their attacks is much higher than the costs entailed.⁵³ Thanks to the combination of their efficiency in approaching targets and their expendability, it seems that women can pose a dangerous security threat to Europe, should they infiltrate the continent.

Furthermore, it could barely be possible for the countries' intelligence agencies to detect to-be attacks, if these women acted independently of one another without leaving any online traces. On the other hand, the above-mentioned example of Hassan cannot be viewed as an exceptional case, but is rather one of the thousands of similar fates. The number of unaccompanied and separated children (UASC) was nearly ten times more than of accompanied ones arriving in Italy by sea in 2016.⁵⁴ A more dramatic parallel could be observed in 2017, since an almost fourteen-fold difference can be witnessed in favour of UASC.⁵⁵ When they leave for abroad, although they distance themselves from their place of origin physically, their close connection to religion remains. This relation might even be strengthened due to experienced exclusion and initial alienation in the foreign land. As a result, there is growing concern about the likelihood of re-radicalisation if these disturbed children might end up in Europe. Discussing the benefits of the Nigerian de-radicalisation program, Fatima Akilu agrees that they 'don't have the resources to reach many of the children in the camps, and they certainly wouldn't get it in Europe'.⁵⁶

Nevertheless, it is important to note that push factors driving migration do not always lead to youth radicalisation. Likewise, push factors driving the radicalisation of young people do not inevitably pave the way for migration either. There is no single component; individuals are rather influenced by the combination of these economic, political, social conditions and/or terrorism in countries where migrants and refugees originate from.⁵⁷ The rise of youth radicalisation in Europe can be held responsible for forging a link between extremism and migration, especially since the latter might open up avenues for terrorist groups to reach their goals. However, the question remains whether these radicalised people could find their way to Europe. A suspected *Boko Haram* member, accused of being involved in hostage-taking and several attacks against villages and schools, was arrested in Germany in 2018.⁵⁸ However, concrete, well-documented evidence and comprehensive further research are needed to prove correlations between radicalisation and migration.

Irregular refugee flows and migration patterns have been exploited to give vent to radicalisation in Kenyan IDP camps.⁵⁹ Similarly, in the Nigerian context, it has been reported that fighters of *Boko Haram* have infiltrated to these camps and flows.⁶⁰ According

⁵³ Galehan, 'Instruments of violence'.

⁵⁴ UNHCR, 'Italy Sea Arrivals Dashboard', December 2016.

⁵⁵ UNHCR, 'Italy Sea Arrivals Dashboard', December 2017.

⁵⁶ Simons, 'Boko Haram jihadists'.

⁵⁷ T Reitano and P Tinti, 'Survive and advance: The economics of smuggling refugees and migrants into Europe', *ISS Paper 289*, November 2015.

⁵⁸ Reuters, 'Suspected Boko Haram attacker arrested in Germany', 26 January 2018.

⁵⁹ S Hellsten, 'Radicalisation and terrorist recruitment among Kenya's youth', *Policy Note No. 1*, The Nordic Africa Institute, February 2016.

⁶⁰ UNHCR, 'Nigeria situation 2017', Supplementary Appeal (Revised July 2017), January–December 2017.

to the Borno State Management Agency (SEMA) ‘at least nine *Boko Haram* insurgents and 100 accomplices were identified among 920 Nigerian refugees who returned from Cameroon’.⁶¹ Disguising themselves as refugees could be beneficial for the Islamist sect for a number of reasons. Firstly, it provides militants an opportunity to perpetrate attacks in closer proximity by pretending to need special medical attention and by the time there is a group of individuals around them, they detonate themselves. Secondly, it strengthens the self-image of the terrorist group as a cunning entity. Lastly, the lack of knowledge about people’s true identity creates an atmosphere of untrustworthiness among the refugees that can easily make suspects of previously-thought victims.⁶²

Refugees and migrants have been in the crosshairs of extremist groups, with terrorist organisations perpetrating direct or indirect attacks. They often take the form of strategic warfare, for instance by striking IDPs or bringing about forced displacement.⁶³ Seeking to answer the question why *Boko Haram* is targeting displaced persons, Kelly Greenhill’s study may prove to be quite useful. She defines coercive engineered migrations as ‘cross-border population movements that are deliberately created or manipulated in order to induce political, military and/or economic concessions from a target state or states’.⁶⁴ In her view, migration can be regarded as a strategic tool possessed by the weak, which is able to manipulate the strong. She argues that after migration has been used by the coercer to spur a conflict, the costs of the coerced in terms of managing the situation can be higher than submitting to the challenger’s demands. Based on this theory, *Boko Haram* could be engineering migration with the intent of both overwhelming its targets’ capacity and destabilising them. It could certainly be an effective strategy considering Nigerian IDPs in the neighbouring countries; however, can the terrorist group constitute a threat to European security?

Following its alignment with ISIL in 2015, there is an increased likelihood that *Boko Haram* could start to be engaged with migrants and refugees besides targeting IDPs.⁶⁵ It appears rather probable in light of ISIL’s renewed strategic focus on European migrants in recent years. Some of the methods they have used were claiming attacks they might not even have been responsible for or more importantly, infiltrating the flows of migrants. It is in the interests of ISIL to depict refugees as individuals capable of posing a security threat to Europe. It is thus absolutely elementary from their perspective that European governments do not view refugees as victims, but rather blur the distinction between them and terrorists.⁶⁶ The truth is that ISIL detests people fleeing their country of origin for Europe, since it completely goes against the message they propagate about the Caliphate being a refuge. If it was truly a safe haven then what could explain the urge of hundreds

⁶¹ News24, ‘Boko Haram fighters found posing as refugees: Nigeria’, 1 July 2017.

⁶² A B Bukarti, ‘Boko Haram: How Perpetrators Impersonate Victims’, *Tony Blair Institute for Global Change*, 21 July 2017.

⁶³ K Koser and A E Cunningham, ‘Migration, Violent Extremism and Terrorism: Myths and Realities’, in *GTI 2015* (Institute for Economics and Peace, 2015).

⁶⁴ K M Greenhill, ‘Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion’, *Strategic Insights* 9, no 1 (2010), 116.

⁶⁵ A-N Mbiyozo, ‘How Boko Haram specifically targets displaced people’, *ISS Policy Brief*, 6 December 2017.

⁶⁶ M Ignatieff, ‘The Refugees & the New War’, *The New York Review*, 17 December 2015.

of thousands of individuals subjecting themselves to a lengthy and dangerous journey instead of remaining there?

In the period of 16–19 September 2015, twelve recordings were circulated with the intention of dissuading migrants and refugees from traveling to Europe by emphasising the high costs and risks associated with the journey. First of all, they stressed that Islamic lands shall not be left, as migrating to ‘infidel territories’ equals to forsaking religion and the Caliphate is the Muslim’s best option for happiness anyway. Secondly, migrants were reminded that as opposed to sharia, the prevalence of human laws awaited them in Europe and refugees would gradually be forced to abandon their religion and convert to Christianity. Additionally, welcoming migrants to Europe was thought to be part of a grand scheme with Europe planning to drain the Muslim population from their countries of origin so that ISIL could be defeated. On top of that, all these irresolvable differences between the Islam world and Europe were illustrated with graphic evidence about the perceived mistreatments of individuals in the continent.⁶⁷

After pledging allegiance to ISIL, there is growing concern that *Boko Haram* could follow suit with focusing its efforts on refugees, infiltrating migration flows and thereby creating a security threat to Europe. Since humanitarian and military support provided to Nigeria seem to be inefficient, Ayoade Olatunbosun-Alakija, Nigeria’s former chief humanitarian coordinator argued that individuals may be triggered to leave the country in case the situation was not dealt with properly and immediately. Fatima Akilu agrees and claims that once hope is lost about the government’s ability to remedy the crisis, a higher number of people could decide that leaving Nigeria might serve their best interests in the long term. She also stated that ‘as *Boko Haram* comes under military pressure, it will no longer see itself as attached to Nigeria, but more connected to other parts of the world through ISIS’.⁶⁸ A potential detachment from Nigeria could save up time and resources that might be channelled to Europe, in which case the terrorist group could constitute a significant threat to European security.

Conclusion

In conclusion we can state that today’s mass migration and terrorism is a sort of a side effect of reactions produced by globalisation. Henceforth, migration and terrorism can never be considered internal problems since they can directly endanger international security. Imbalance, poverty, dictatorship’s expansionary ambition and the relevant cultural background serve as fertile ground to expand terrorism. It is a universal threat. Scales of attacks, qualitative and quantitative indicators of global losses, along with transnational, professional, mobile and unscrupulous terrorist organisations are evident and signify dangers to the overall security of every nation state.⁶⁹

⁶⁷ A Zelin, ‘Targeting Europe’s Refugees Is Not the Answer’, Policy Analysis, *Policy Watch* 2524, The Washington Institute for Near East Policy, 16 November 2015.

⁶⁸ Simons, ‘Boko Haram jihadists’.

⁶⁹ Babos, *The Five Central Pillars*.

Bearing in mind the universal evidences on migration and terrorism, responding to the question whether *Boko Haram* constitutes a threat to European security is not as clear-cut as one might think at first glance. On the one hand, we could argue that the terrorist group *cannot* constitute a European security threat, since the majority of Nigerians arriving in Europe seemingly decided to flee their country of origin due to economic reasons. Furthermore, studying the names of refugees and migrants, it appears to be evident that most of the people originate from the southern part of Nigeria.⁷⁰ However, as argued above, migration is not motivated by a single, separate component, but is rather influenced by a wide variety of push factors embedded in various processes, including political, religious and social factors. Although terrorism in the form of religious and political insurgencies could also be considered a push factor, it would have to be complemented with additional context-dependent elements. Besides, there have only been alleged cases of radicalised individuals traveling to Europe. Concrete, well-documented evidence and comprehensive further research are needed to prove correlations between radicalisation and migration.

On the other hand, we can also find evidence that *Boko Haram* can pose a threat to European security, which might be attested by the terrorist organisation's increased use of women as soft targets for committing suicide attacks and the potential re-radicalisation of traumatised children in Europe. Both of these trends can be rather perilous in case these people truly infiltrate the continent; the former in light of women's ability to access camps more easily and get close to their targets without arousing much suspicion, the latter due to the youth's receptiveness to radicalisation and/or religious indoctrination. Furthermore, pledging allegiance to ISIL in 2015 raises the question if *Boko Haram* will follow in the footsteps of Daesh, placing the strategic emphasis on refugees and migrants instead of dealing with IDPs. If so, infiltrating to European refugee flows with the intent of perpetrating attacks in the continent at a later time appears to be the next step. It would certainly increase European governments' level of cautiousness, paving the way for viewing migrants as a security threat.

However, the gradual and constant decrease in the influx of Nigerian migrants from 2018 to the present can be justified by the aspirations of European governments that are meant to limit and more strictly monitor the number of refugees arriving in Europe from Africa. While global security is of utmost importance, it is 'necessary to balance [security-intense responses] against humanitarian concerns and international human rights standards'.⁷¹ As a consequence, challenges should be addressed through continuous cooperation between African and European governments, and although international support is needed, local forces also play a pivotal role in equipping Africans with technical and educational skills as well as providing jobs for them on a regional, national or even continental level.⁷² Considering the pace and intensity of migration, these collaborations seemed to have come to fruition, since a significant decrease could be observed in the

⁷⁰ O'Grady, 'Nigerian Migrants'; BBC, 'A Nigerian's nightmare'; Agbakwuru, 'FG inaugurates'.

⁷¹ Cachalia et al., 'The dynamics of youth radicalisation', 14.

⁷² A P Garcia and I Martin, 'EU cooperation with third countries in the field of migration', Directorate-General for Internal Policies, Policy Department, Citizens' Rights and Constitutional Affairs, European Parliament, 2015.

number of African migrants and refugees coming to Europe recently.⁷³ If continuous cooperation is to remain, chances are slim that *Boko Haram* could constitute a threat to European security.

References

- Agbakwuru, J, 'FG inaugurates Migration Centre in Edo'. *The Vanguard Nigeria*, 07 March 2018. Online: www.vanguardngr.com/2018/03/fg-inaugurates-migration-centre-edo
- Agbiboa, D E, 'The Nigerian burden: religious identity, conflict and the current terrorism of Boko Haram'. *Conflict, Security & Development* 13, no 1 (2013), 1–29. Online: <https://doi.org/10.1080/14678802.2013.770257>
- Aghedo, I and S J Eke, 'From Alms to Arms: The *Almajiri* Phenomenon and Internal Security in Northern Nigeria'. *The Korean Journal of Policy Studies* 28, no 3 (2013), 97–123.
- Akubo, J, 'Boko Haram: Army unveils operation 'deep punch' for final push'. *The Guardian Nigeria*, 9 July 2017. Online: www.guardian.ng/news/boko-haram-army-unveils-operation-deep-punch-for-final-push/
- Amnesty International, 'Lake Chad region: Boko Haram's renewed campaign sparks sharp rise in civilian deaths', 05 September 2017. Online: www.amnesty.org/en/latest/news/2017/09/lake-chad-region-boko-harams-renewed-campaign-sparks-sharp-rise-in-civilian-deaths/
- Babos, T, *The Five Central Pillars of European Security*. Brussels: NATO Public Diplomacy Division, Budapest: Strategic and Defense Research Center, Oberammergau: NATO School, Budapest: Chartapress, 2007. Online: www.files.ethz.ch/isn/56271/07_Babos.pdf
- Barungi, B, O Odhiambo and R Asogwa, *African Economic Outlook 2017: Nigeria*. African Development Bank, OECD Development Centre, UNDP, 2017. Online: www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/AEO_2017_Report_Full_English.pdf
- BBC, 'Boko Haram in Nigeria: Abu Musab al-Barnawi named as new leader', 03 August 2016. Online: www.bbc.com/news/world-africa-36963711
- BBC, 'A Nigerian's nightmare failed bid to migrate to Europe', 28 April 2017. Online: www.bbc.com/news/world-africa-39731109
- BBC, 'Migrant crisis: Italy minister Salvini closes ports to NGO boats', 30 June 2018. Online: www.bbc.com/news/world-europe-44668062
- BBC, 'Nigeria's Katsina school abduction: Boko Haram says it took the students', 15 December 2020. Online: www.bbc.com/news/world-africa-55295701
- Besenyő, J, 'Fences and Border Protection: The Question of Establishing Technical Barriers in Europe'. *AARMS* 16, no 1 (2017), 77–87. Online: http://real.mtak.hu/83717/1/aarms_2017_1_07_besenyő.original_u.pdf
- Bloom, M, *Dying to Kill: The Allure of Suicide Terror*. New York: Columbia University Press, 2005.

⁷³ BBC, 'Migrant crisis: Italy minister Salvini closes ports to NGO boats', 30 June 2018; UNHCR, 'Italy Sea Arrivals Dashboard', December 2018; UNHCR, 'Italy Sea Arrivals Dashboard', December 2019; UNHCR, 'Italy Sea Arrivals Dashboard', October 2020.

- Bloom, M, 'Female suicide bombers: a global trend'. *Daedalus* 136, no 1 (2007), 94–102. Online: <http://doi.org/10.1162/daed.2007.136.1.94>
- Bloom, M, 'Bombshells: Women and Terror'. *Gender Issues* 28, no 1 (2011), 1–21. Online: <http://doi.org/10.1007/s12147-011-9098-z>
- Botha, A, 'Radicalisation in Kenya: Recruitment to al-Shabaab and the Mombasa Republican Council', *ISS Paper* 265, September 2014. Online: <https://issafrica.s3.amazonaws.com/site/uploads/Paper265.pdf>
- Bukarti, A B, 'Boko Haram: How Perpetrators Impersonate Victims', *Tony Blair Institute for Global Change*, 21 July 2017. Online: www.institute.global/policy/boko-haram-how-perpetrators-impersonate-victims
- Burpee, J, 'A Deadly Journey: Desert, Sea, Detention...On the Road to Europe'. *IOM*, September 2017. Online: <http://features.iom.int/stories/deadly-journey/>
- Cachalia, R C, U Salifu and I Ndung'u, 'The dynamics of youth radicalisation in Africa: Reviewing the current evidence'. *ISS Paper* 296, August 2016. Online: <https://issafrica.s3.amazonaws.com/site/uploads/paper296-1.pdf>
- Campbell, J, 'Nigeria Security Tracker'. *Council on Foreign Relations*, 12 October 2020. Online: www.cfr.org/nigeria/nigeria-security-tracker/p29483
- Dalton, A and V Asal, 'Is It Ideology or Desperation: Why Do Organizations Deploy Women in Violent Terrorist Attacks?' *Studies in Conflict & Terrorism* 34, no 10 (2011), 802–819. Online: <http://doi.org/10.1080/1057610X.2011.604833>
- Davis, J, *Women in Modern Terrorism: From Liberation Wars to Global Jihad and the Islamic State*. Lanham: Rowman & Littlefield Publishers, 2017.
- DTM, 'Libya's Migrant Report', *Flow Monitoring*, Round 17, January–February 2018. Online: <https://displacement.iom.int/system/tdf/reports/DTM%20Libya%20Round%2017%20Migrant%20Report%20%28Jan-Feb%202018%29%281%29.pdf?file=1&type=node&id=3106>
- European Commission, Standard Eurobarometer 89 – Wave EB89.1. Kantar Public Brussels on behalf of TNS opinion & social, Survey requested and co-ordinated by the European Commission, Directorate-General for Communication, Fieldwork, March 2018.
- Eurostat, 'Asylum and new asylum applicants: monthly data', 2018. Online: <https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00189&plugin=1>
- Felter, C, 'Nigeria's Battle with Boko Haram', *Council on Foreign Relations*, 08 August 2018. Online: www.cfr.org/background/nigerias-battle-boko-haram
- Flint, C, *Introduction to Geopolitics*. New York: Routledge, 2011. Online: <https://doi.org/10.4324/9780203816752>
- Gaffey, C, 'Why are over 1 million displaced persons in Nigeria too scared to go home?' *Newsweek*, 12 October 2017. Online: www.newsweek.com/boko-haram-idps-refugees-nigeria-683001
- Galehan, J, 'Instruments of violence: Female suicide bombers of Boko Haram'. *International Journal of Law, Crime and Justice* 58 (2019), 113–123. Online: <https://doi.org/10.1016/j.ijlcrj.2019.04.001>
- Garcia, A P and I Martin, 'EU cooperation with third countries in the field of migration', Directorate-General for Internal Policies, Policy Department, Citizens' Rights and

- Constitutional Affairs, European Parliament, 2015. Online: www.europarl.europa.eu/RegData/etudes/STUD/2015/536469/IPOL_STU%282015%29536469_EN.pdf
- Greenhill, K M, 'Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion'. *Strategic Insights* 9, no 1 (2010). Online: <https://doi.org/10.7591/9780801458668>
- GTI, *Measuring and Understanding the Impact of Terrorism*. Institute for Economics and Peace, 2015. Online: www.visionofhumanity.org/wp-content/uploads/2020/10/2015-Global-Terrorism-Index-Report.pdf
- GTI, *Measuring and Understanding the Impact of Terrorism*. Institute for Economics and Peace, 2016. Online: www.economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf
- Hellsten, S, 'Radicalisation and terrorist recruitment among Kenya's youth'. *Policy Note No. 1*, The Nordic Africa Institute, February 2016. Online: <http://nai.diva-portal.org/smash/get/diva2:906144/FULLTEXT01.pdf>
- Hooper, K, 'European Leaders Pursue Migration Deals with North African Countries, Sparking Concerns about Human Costs'. *Migration Policy Institute*, 17 December 2017. Online: www.migrationpolicy.org/article/top-10-2017-issue-3-european-leaders-pursue-migration-deals-north-african-countries
- Human Development Report, *The next frontier: Human development and the Anthropocene*. New York: UNDP, 2020. Online: <http://hdr.undp.org/sites/default/files/hdr2020.pdf>
- Ignatieff, M, 'The Refugees & the New War', *The New York Review*, 17 December 2015. Online: www.nybooks.com/articles/2015/12/17/refugees-and-new-war/
- Inyang, I, 'Boko Haram is broke – UN Envoy'. *Daily Post*, 08 February 2017. Online: <https://dailypost.ng/2017/02/08/boko-haram-broke-un-envoy/>
- IOM, 'Migration Trends Across the Mediterranean: Connecting the Dots', *Altai Consulting for IOM MENA Regional Office*, June 2015. Online: https://publications.iom.int/system/files/altai_migration_trends_across_the_mediterranean.pdf
- IOM, 'World Migration Report 2018'. Online: www.iom.int/sites/default/files/country/docs/china/r5_world_migration_report_2018_en.pdf
- IOM UN Migration, 'Mediterranean Migrant Arrivals Reach 110,833 in 2018; Deaths Reach 2,160', 12 November 2018. Online: <https://reliefweb.int/sites/reliefweb.int/files/resources/Mediterranean%20Migrant%20Arrivals%20Reach%20110.pdf>
- Isike, C and E Isike, 'Migration and the geopolitics of Boko Haram terrorism in Nigeria'. *Strategic Review for Southern Africa* 40, no 2 (2018), 34–51. Online: <https://doi.org/10.35293/srsa.v40i2.183>
- Koser, K and A E Cunningham, 'Migration, Violent Extremism and Terrorism: Myths and Realities', in *GTI 2015*. Institute for Economics and Peace, 2015. Online: www.files.ethz.ch/isn/194968/Global-Terrorism-Index-2015.pdf
- Ladbury, S, H Allamin, Ch Nagarajan, P Francis and U O Ukiwo, 'Jihadi Groups and State-Building: The Case of Boko Haram in Nigeria'. *Stability: International Journal of Security & Development* 5, no 1 (2016), 1–19. Online: <https://doi.org/10.5334/sta.427>
- Loada, A and P Romaniuk, 'Preventing Violent Extremism in Burkina Faso: Toward National Resilience Amid Regional Insecurity'. *Global Center on Cooperative Security*, June

2014. Online: www.globalcenter.org/wp-content/uploads/2014/07/BF-Assessment-Eng-with-logos-low-res.pdf
- Mahmood, O S, 'More than propaganda: A review of Boko Haram's public messages'. *ISS, West Africa Report* 20, March 2017. Online: <https://issafrica.s3.amazonaws.com/site/uploads/war20.pdf>
- Mahmood, O S, 'Boko Haram in 2016: A highly adaptable foe'. *ISS Today*, 07 February 2017.
- Mark, M, 'Boko Haram vows to fight until Nigeria establishes sharia law'. *The Guardian*, 27 January 2012. Online: www.theguardian.com/world/2012/jan/27/boko-haram-nigeria-sharia-law
- Mbiyozo, A-N, 'How Boko Haram specifically targets displaced people'. *ISS Policy Brief*, 6 December 2017. Online: <https://issafrica.s3.amazonaws.com/site/uploads/policybrief109.pdf>
- Mercy Corps, 'Motivations and Empty Promises: Voices of Former Boko Haram Combatants and Nigerian Youth', April 2016. Online: www.mercycorps.org/sites/default/files/2019-11/Motivations%20and%20Empty%20Promises_Mercy%20Corps_Full%20Report_0.pdf
- Moten, A R, 'Understanding Terrorism: Contested Concept, Conflicting Perspectives and Shattering Consequences'. *Intellectual Discourse* 18, no 1 (2010), 35–63.
- NBS, '2019 Poverty and Inequality in Nigeria: Executive Summary'. *National Bureau of Statistics*, 2019. Online: <https://nigerianstat.gov.ng/>
- News24, 'Boko Haram fighters found posing as refugees: Nigeria', 1 July 2017. Online: www.news24.com/news24/Africa/News/boko-haram-fighters-found-posing-as-refugees-nigeria-20170701
- O'Grady, S, 'Nigerian Migrants Get a Welcome Home. Jobs Are Another Story'. *New York Times*, 08 January 2018. Online: www.nytimes.com/2018/01/08/world/africa/migrants-nigeria-libya.html
- Okeyim, M O, *The State and Migration of Nigerians into the European Union to Live in Spain*. Doctoral thesis, University of Alicante, 2012. Online: https://rua.ua.es/dspace/bitstream/10045/28375/1/Tesis_Okiri_Okeyim.pdf
- Pettiford, L and D Harding, *Terrorism: The New World War*. London: Arcturus Publishing Limited, 2003.
- Pew Research Center, 'At Least a Million Sub-Saharan Africans Moved to Europe Since 2010', 22 March 2018. Online: www.pewresearch.org/global/2018/03/22/at-least-a-million-sub-saharan-africans-moved-to-europe-since-2010/
- Poushter, J, 'In nations with significant Muslim populations, much disdain for ISIS', *Pew Research Center*, 17 November 2015. Online: www.pewresearch.org/fact-tank/2015/11/17/in-nations-with-significant-muslim-populations-much-disdain-for-isis/
- Ranstorp, M, 'Terrorism in the Name of Religion'. *Journal of International Affairs* 50, no1 (1996), 41–62.
- Reitano, T and P Tinti, 'Survive and advance: The economics of smuggling refugees and migrants into Europe'. *ISS Paper* 289, November 2015. Online: <https://issafrica.s3.amazonaws.com/site/uploads/Paper289-2.pdf>
- Reuters, 'Suspected Boko Haram attacker arrested in Germany', 26 January 2018. Online: www.reuters.com/article/us-nigeria-security-germany-idUSKBN1FF1X4

- Simons, J W, 'Boko Haram jihadists 'set to infiltrate Europe through Libya' as Nigeria's humanitarian crisis threatens NEW WAVE of illegal migration'. *MailOnline*, 13 February 2018. Online: www.dailymail.co.uk/news/article-5382499/Boko-Haram-jihadists-infiltrate-Europe-Libya.html
- The Sun, 'Boko Haram allegedly split over leadership', 17 July 2018. Online: www.sunnewsonline.com/shekau-boko-haram-split-leadership/
- UNHCR, 'Italy Sea Arrivals Dashboard', December 2016. Online: <https://data2.unhcr.org/en/documents/details/53356>
- UNHCR, 'Italy Sea Arrivals Dashboard', December 2017. Online: <https://data2.unhcr.org/en/documents/details/61547>
- UNHCR, 'Nigeria situation 2017', Supplementary Appeal (Revised July 2017), January–December 2017. Online: https://reporting.unhcr.org/sites/default/files/Revised%202017%20SB%20Nigeria%20Situation_FINAL.pdf
- UNHCR, 'Italy Sea Arrivals Dashboard', December 2018. Online: <https://data2.unhcr.org/en/documents/details/67555>
- UNHCR, 'Italy Sea Arrivals Dashboard', December 2019. Online: <https://data2.unhcr.org/en/documents/details/73536>
- UNHCR, 'Italy Sea Arrivals Dashboard', October 2020. Online: <https://data2.unhcr.org/en/documents/details/83169>
- UNHCR, 'Nigeria emergency', 2020. Online: www.unhcr.org/nigeria-emergency.html
- Weber, H, 'Can Violent Conflicts Explain the Recent Increase in the Flow of Asylum Seekers From Africa Into Europe?' *Journal of Immigrant & Refugee Studies* 17, no 4 (2019), 405–424. Online: <https://doi.org/10.1080/15562948.2018.1517424>
- Zelin, A, 'Targeting Europe's Refugees Is Not the Answer', Policy Analysis, *Policy Watch* 2524, The Washington Institute for Near East Policy, 16 November 2015. Online: www.washingtoninstitute.org/policy-analysis/targeting-europes-refugees-not-answer

Military Intervention and Changing Balance of Power in Libya:

A Strongman, Russian Mercenaries and Turkish Drones¹

Péter SELJÁN² 

Libya has sunk into chaos since Muammar Gaddafi was deposed by a Western-led military intervention in 2011. Since then, the Libyan crisis has escalated into an internationalised armed conflict, and a major power struggle between Turkey, Qatar, Italy, and Russia, Egypt, France, and the United Arab Emirates. In the last few years, General Khalifa Haftar has become Libya's most prominent military commander, who is now ruling the eastern part of the country, as the head of the Libyan National Army. His military offensive, launched in April 2019, to capture the capital Tripoli forced Turkey to help the UN-backed Government of National Accord to avoid defeat. But Haftar too received additional military support, especially from Abu Dhabi and Moscow. This escalated the conflict even further, spurring Ankara for another, this time more consequential intervention, which was able to change the local balance of power, so diplomatic efforts and the peace process could get another chance.

Keywords: *Libya, civil war, intervention, balance of power, Turkey, Russia*

Introduction

The internationalisation of Libya's conflict began with the North Atlantic Treaty Organization's 2011 intervention, while in addition, there were also rival interventions by Qatar and the United Arab Emirates to assist Libyan revolutionary militias, though those were less recognised at that time. Libya's strategic location at the Maghreb, its significant oil and gas reserves and its revolutionary upheaval made Libya's crisis an attractive opportunity for outside actors, while in fact, the country's post-revolutionary decline, increasing fragmentation and state collapse represents an ever-growing international

¹ Supported by the ÚNKP-20-4-I new national excellence program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

² PhD candidate, Corvinus University of Budapest, International Relations; e-mail: peter@seljan.hu

security threat.³ It seems that in the middle of this general upheaval, one of the major players, General Khalifa Haftar was not able to become the leader who could defeat the UN-recognised Government of National Accord (GNA) and its forces. He rather serves largely as a proxy for the external actors like Russia, and as such, Haftar has acted deliberately as an obstacle to the much needed stabilisation, up until the end of 2020.⁴

The conflict took an encouraging positive turn in August 2020, when the head of the Tripoli-based GNA, Fayez al-Sarraj announced a ceasefire and called for parliamentary and presidential elections to be held in 2021. Aguila Saleh, speaker of the rival eastern-based, pro-Haftar House of Representatives, also called on all parties to adhere to the truce, which could prevent further foreign military intervention in Libya.⁵ Finally, in October, the warring factions have signed an agreement on a permanent ceasefire, after five days of UN-brokered talks in Geneva, which can serve as an important starting point towards potentially long-lasting peace in Libya.⁶ However, this was only partially possible because of previous Turkish intervention on the western side, which tilted the balance of power to the GNA's favour, thus preventing Haftar from marching westwards.⁷

The stabilisation of Libya has key importance for the security of the region and for Europe, partly since the oil-rich nation is a key transit point for migrants heading to the European Union from Africa. However, the Libyan civil war has not received that much attention in recent years that it would deserve. In this paper we summarise the most important developments of the last two years of the conflict (2019–2020), pointing out how the local balance of power changed through the military intervention of Russia and Turkey. In the first part, we give a short introduction of General Khalifa Haftar, as a central player of the conflict. Then we discuss his offensive against Tripoli, the Russian support he received and the Turkish interventions on the side of the internationally recognised government that turned the fight for the capital. In the end, we close our paper with drawing some conclusions.

Who is Haftar?

After Haftar announced his offensive against Tripoli, the general's name appeared more frequently in the mainstream media, and many news outlets published short profiles and bios on him. According to the BBC, Khalifa Haftar was born in Libya in 1943, and he was one of the group of officers led by Colonel Muammar Gaddafi who staged a coup and

³ Foreign actors involved in Libya include the United Arab Emirates, Egypt, France, Russia, the United States, Saudi Arabia, Sudan, Jordan, Turkey, Qatar and Italy. See Ramy Allahoum, 'Libya's war: Who is supporting whom', *Al Jazeera*, 09 January 2020.

⁴ Tarek Megerisi, 'Geostrategic Dimensions of Libya's Civil War', *Africa Security Brief* No 37, May 2020, 1–2.

⁵ The Guardian, 'UN-supported Libya government and rival authority call ceasefire', 21 August 2020.

⁶ Nick Cumming-Bruce and Declan Walsh, 'Libya Cease-Fire Raises Hopes for Full Peace Deal', *The New York Times*, 23 October 2020.

⁷ By 2015, Libya was practically divided into parts corresponding to the former historical regions (administrative divisions) of the country. The most populous region is Tripolitania in the west with a population of approximately 3.5 million, followed by eastern Cyrenaica with around 1.5 million and the poorest region is Fezzan in the south with a population less than 500 thousand.

seized power from King Idris in 1969. Then, Haftar oversaw the Libyan forces involved in the conflict in Chad in the 1980s. But as Libya was defeated by the French-backed Chadian forces, Haftar and his few hundred men were captured by the Chadians in 1987. Gaddafi denied the presence of Libyan troops in Chad, and even disowned Haftar, which led the general to devote his time to toppling the Libyan leader. He went into exile in the United States, but during this time, he was in close cooperation with the CIA, which backed him in several attempts to assassinate Gaddafi. After the start of the so-called Arab Spring protests in 2011, Haftar returned to Libya, where he became the commander of the rebels in the east.⁸

As Tarek Megerisi highlighted, the collapse of the General National Congress (GNC) in the Spring of 2014 was a turning point in Libya's transition, symbolised best by the re-emergence of General Haftar who faded into obscurity until February 2014. In 2011, he was quickly sidelined, since many Libyans were unwilling to work with him, deeming him responsible for atrocities committed during the Chadian war of the 1980s. In February 2014, Haftar unexpectedly appeared on TV to outline his plan to save the nation and called on Libyans to revolt against the elected GNC, whose mandate was still valid at the time. According to Megerisi, Haftar's TV announcement represented the beginning of politics by other means in Libya: 'The moving away from politicians employing militias toward a paradigm whereby militias employed politicians to provide a shroud of legitimacy.' Haftar's reintroduction to Libya was backed by Cairo, and while his coup attempt failed to gain support in the capital Tripoli, he quickly provided a new reason for some other actors to cooperate with him over the course of 2014, by launching a war on terror in eastern Libya.⁹

As Jon Lee Anderson of *The New Yorker* noted, 'Haftar has fought with and against nearly every significant faction in the country's conflicts, leading to a reputation for unrivalled military experience and for a highly flexible sense of personal allegiance'. In Operation Dignity, the Libyan National Army, led by Haftar, has taken much of the eastern half of Libya, while most of the remainder was held by Libya Dawn, a loose coalition of militias. Anderson met with Haftar in person, and the general told him why he had gone back to Libya. After participating in the 2011 uprising against Gaddafi, Haftar tried to find a place for himself in the country's new political landscape. When he did not succeed, he returned to the U.S. from where he watched as Libya floundered under a succession of weak governments, and the country's militias grew more powerful. This turn of events upset Haftar, who soon became the self-declared saviour of Libya. But while Haftar said he was targeting terrorists, his definition of terrorism is way too broad, and many consider him a vigilante. Thus, it is possible that Haftar's vigilantism will motivate those who oppose him to unite, giving a common cause to extremists and non-extremists alike, next to the fight against the Islamic State. One of the main legacies of the history of tribalism in Libya, and partly the decades long rule of Gaddafi, is that things can get settled only by force, which has created a Libyan culture of 'with or against'.¹⁰

⁸ BBC, 'Khalifa Haftar: The Libyan general with big ambitions', 08 April 2019.

⁹ Megerisi, 'Geostrategic Dimensions', 3–4.

¹⁰ Jon Lee Anderson, 'The Unravelling', *The New Yorker*, 16 February 2015.

Haftar's Tripoli offensive

As the war on terror gradually ended, Haftar's foreign backers provided him the support needed to extend his reach further to acquire Libya's oil export terminals and to conquer the remainder of eastern Libya. Meanwhile, thanks to his foreign allies, Haftar refused to support the UN-backed Libyan Political Agreement (LPA), which was intended to reunify the country, establishing the Government of National Accord in December 2015, led by a new Prime Minister, Fayeze al Sarraj.¹¹ This peace process was backed by the United States, the United Kingdom and Italy, hoping that it could end Libya's civil war and create a partner for combatting terrorism and tackling migration. However, as the process dragged on, the crisis just deepened. Sarraj and his government arrived in Tripoli in March 2016, when it has become evident that the GNA lacks real political power, struggled to operate in a city controlled by militias and the international actors quickly abandoned it for more expedient policies. Haftar ultimately declared the Libyan Political Agreement void in December 2017.¹² UN Special Representative Ghassan Salame tried to break the diplomatic deadlock during the next two years to create a new, inclusive political process that would lead to a new government and institutions more reflective of Libya's patchwork of political and military actors. However, the new plan remained highly contested with many in Libya refusing to support it, which eroded the credibility of the international actors in the country. Eventually, this led to Haftar trying to seize power by launching a surprise attack on Tripoli in April 2019.¹³ After these, events have accelerated, but it does worth going through the timeline of the next months.¹⁴

On April 7, GNA forces announced a counter-offensive against Haftar's forces, aimed at 'purging all Libyan cities of aggressor and illegitimate forces'. The Wall Street Journal reported on April 12, that days before Haftar launched the offensive, Saudi Arabia offered tens of millions of dollars to help pay for the operation. The offer, which Haftar accepted, allegedly came during a visit by Haftar to Riyadh, and was intended to buy the loyalty of tribal leaders, recruit and pay fighters, and for other military purposes.¹⁵ The White House released a statement on April 19, saying that U.S. President Donald Trump recognises Haftar's significant role in fighting terrorism and securing Libya's oil resources, which prompted thousands of people to take to the streets in Tripoli, calling on the international community to stop the military aggression by Haftar's forces.¹⁶ On May 22, Ghassan Salame, the UN envoy to Libya, denounced the conflict raging in Libya, highlighting that the country has become a textbook example of foreign intervention in local conflicts.¹⁷ But on May 26, Haftar said in an interview that he will continue fighting until militias in Tripoli laid down their arms, even though his objective is to reach a political solution.¹⁸

¹¹ Aziz El Yaakoubi, 'Libyan factions sign U.N. deal to form unity government', *Reuters*, 17 December 2015.

¹² Al Jazeera, 'Haftar: Libya's UN-backed government's mandate obsolete', 18 December 2017.

¹³ Megerisi, 'Geostrategic Dimensions', 4–6.

¹⁴ Al Jazeera, 'Timeline: Haftar's months-long offensive to seize Tripoli', 19 February 2020.

¹⁵ Jared Malsin and Summer Said, 'Saudi Arabia Promised Support to Libyan Warlord in Push to Seize Tripoli', *The Wall Street Journal*, 12 April 2019.

¹⁶ Al Jazeera, 'Trump praises Haftar in apparent reversal of US policy on Libya', 20 April 2019.

¹⁷ Al Jazeera, 'UN envoy: 'Libya a textbook example of foreign intervention'', 23 May 2019.

¹⁸ Al Jazeera, 'Libya's Haftar vows to fight until Tripoli 'militias' defeated', 26 May 2019.

Haftar's Tripoli offensive and his plan to take power in April 2019 failed eventually, as he found himself confronted by the greatest mobilisation of fighters in the country since the 2011 revolution against Gaddafi.

On June 29, Haftar banned Turkish commercial flights to the GNA and ordered LNA forces to attack Turkish ships and interests in the country, which signalled that the tensions between the GNA-supporter Ankara and Haftar are increasing. On July 1, LNA's air force destroyed a Turkish drone parked at Mitiga International Airport, while Turkey's foreign ministry accused Haftar's forces of seizing six of its citizens. Ankara issued a warning to Haftar, urging him to release the Turkish citizens, or the LNA will become a 'legitimate target'. The warring sides agreed to a temporary truce on August 10, which was proposed by the UN during the Muslim holiday of Eid al-Adha. Eventually, in November, a UN report revealed that the United Arab Emirates, Sudan, Turkey and Jordan have been violating the arms embargo in Libya.¹⁹ In the middle of November, the U.S. has finally called on Haftar to stop his months-long offensive on Tripoli and said it would back the GNA's forces against Russia's attempts to exploit the conflict. This was the most explicit call by the U.S. against Haftar, who was earlier praised by President Trump.²⁰ A week later, on November 23, Haftar declared a 'no-fly zone' in the skies over the capital Tripoli, drawing a warning from the GNA. But the events took a major turn on November 27, when Turkey and Libya signed two agreements on security and military cooperation and restriction of marine jurisdictions.²¹ On December 5, GNA officials announced that they will confront Moscow over the alleged deployment of Russian mercenaries to fight alongside Haftar's forces, saying that they documented between 600 and 800 Russian mercenaries in Libya, while on December 22, Turkish President Recep Tayyip Erdoğan said that Turkey will increase its military support to the GNA if necessary.²²

Haftar's offensive could not succeed as his forces struggled to maintain long supply lines through territory that they barely controlled. However, after the decision was made to launch the offensive, there were no other choices left for General Haftar and his supporters. He either had to win the conflict and establish himself as the new ruler of Libya, or lose everything, and let a new chapter begin for the country. And this situation mobilised not just Libyans, but foreign actors as well, especially Russia and Turkey. According to Megerisi, Russia has long used the Libyan civil war to advance its relationships with Egypt and the UAE, while simultaneously expanding its influence in the Mediterranean and its access to Libya's natural resources. As he noted, 'Russia pulled a page from its Syria playbook to prop up a weak and isolated authoritarian leader in a conflict most global actors wanted to avoid'.²³ Libya's destabilisation created opportunities for Russia to increase its influence in the region, and ensuring Moscow played a decisive role in any future political settlement.

¹⁹ 'Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011)', *United Nations Security Council*, S/2019/914, 09 December 2019.

²⁰ 'Joint Statement on U.S.–Libya Security Dialogue', *U.S. Department of State*, 14 November 2019.

²¹ Al Jazeera, 'Libya, Turkey sign deals on security and maritime jurisdictions', 28 November 2019.

²² Al Jazeera, 'Timeline: Haftar's months-long offensive'.

²³ Megerisi, 'Geostrategic Dimensions', 6.

Turkey turns the fight

Before the Arab Spring, Turkey secured a major share of the construction contracts in Libya. In addition, Ankara and Tripoli had agreed to increase their investments in the energy sector, small and medium-sized enterprises, technology, agriculture and so on. As a result, there were around 25,000 Turkish employees in Libya by 2011, and Turkish investors spent billions of dollars in the construction sector.²⁴ In light of its economic interests in Libya, it is understandable why Turkey first opposed the military intervention against Gaddafi in the spring of 2011. But Ankara soon realised that the Turkish position cannot be upheld, thus finally gave in, and supported the Libyan intervention. Up until 2014, Turkey strove to restore its economic relationship with Libya, supported the stabilisation efforts and the establishment of a central government. Ankara supported the Libyan political agreement signed in December 2015, and the establishment of the UN-backed Government of National Accord as well. The Turkish military role supporting the GNA grew as the tension increased on the ground, especially after Haftar's offensive against Tripoli in April 2019.²⁵

Since Turkey has long maintained economic interests in Libya, and Haftar's eventual success would cement Emirati and Egyptian influence in North Africa, as long as Haftar has foreign backing and the capabilities to wage war on the GNA, he presents a serious challenge for Turkey in Libya and in the region. For this reason, Haftar's Tripoli offensive forced Turkey to either move against Haftar and his foreign supporters (namely the UAE, Egypt and Russia) to claim Libya, or to let go of the GNA's hand. It also must be noted that this situation provided Turkey an opportunity to advance its economic interests in the eastern Mediterranean. In February 2018, significant gas reserves have been discovered in that area, and a coalition formed between Greece, Cyprus, Israel and Egypt to begin to develop security and economic infrastructure, which Turkey viewed as a direct threat to its economic interests and dominant security role in the region.²⁶

Turkey joined the war in May 2019, on the side of the GNA, though its military support in that time was mainly unannounced and clandestine. Turkish military support began to take a public character when the GNA had received a shipment of armoured vehicles and arms after asked its ally Turkey for help.²⁷ In June, President Erdoğan announced that Turkey was providing weapons to the GNA under an unspecified military cooperation agreement, and he also added that Ankara's military support allowed Tripoli to 'restore balance' in Libya against Haftar's forces backed by the UAE and Egypt.²⁸ But the Turkish military support principally consisted of just a small drone fleet and armoured personnel

²⁴ Ferhat Polat, 'The trajectory of Turkey-Libya relations', *TRT World*, 30 August 2019.

²⁵ 'Turkey's Growing Role in Libya: Motives, Background and Responses', *Arab Center for Research & Policy Studies*, 15 January 2020, 1.

²⁶ Michael Tanchum, 'A dangerous policy of Turkish containment in the Eastern Mediterranean', *The Jerusalem Post*, 10 July 2019.

²⁷ Reuters, 'Forces loyal to Libya's U.N.-backed government receive military hardware', 18 May 2019.

²⁸ 'Turkey's Growing Role in Libya', 1.

carriers. Thus, the net effect of this equipment on the battle was limited and overall, the Turkish aid was not as decisive nor as substantial as the GNA might have hoped.²⁹

While Abu Dhabi, Cairo, Ankara and Doha have been supporting the competing sides of the Libyan conflict from its early stages, the civil war escalated further in the fall of 2019 with the deployment of foreign mercenaries in support of Haftar's forces. By the fall of 2019, diminishing Turkish support had shifted the momentum to the LNA, which was mainly due to the increase of Emirati support and Chinese-designed Wing Loong II combat drones, but also due to yet another foreign intervention into the conflict. In the fall of 2019, hundreds of Russian paramilitary fighters and mercenaries from the Kremlin-linked Wagner Group, arrived to help the LNA forces fighting for the capture of Tripoli, which tilted the balance of the conflict in Haftar's favour.³⁰ The Wagner Group fighters took on an increasingly active role in the LNA advance on the capital, supported by the UAE, and as a result of this foreign support, Haftar's forces steadily gained territory in late 2019. At the end of the year, for the first time since the start of the 2019 war, the prospect of an LNA push into central Tripoli appeared as a real possibility. But while facilitating these advances, Russia had inadvertently spurred another round of foreign military intervention in Libya, arguably the most consequential since 2011.³¹

Fearing a potential collapse of its defences around Tripoli, the UN-backed GNA in the late fall of 2019 turned again to Turkey for help. As a result, on November 27, the GNA and Ankara signed two memoranda of understanding relating to security and military cooperation, and the definition of maritime jurisdiction areas, the latter of which was basically a deal on an exclusive economic zone in the eastern Mediterranean that would grant Turkish exploration and drilling rights to offshore hydrocarbon resources.³² In return, President Erdoğan promised closer security cooperation and to send military support to the GNA. Two weeks after the activation of the maritime border demarcation agreement, the security and military cooperation agreement with Libya was also approved by the Turkish parliament.³³ This agreement with Libya was a major power play, which aligned with Turkish strategic goals in the Mediterranean region as well as Turkey's economic penetration into Africa.³⁴ More importantly, this agreement significantly transformed the Libyan war, opening a new chapter in the history of the conflict. Turkish military support to the GNA from this point became open and more serious. Turkey so far has sent military advisers, arms and a fleet of 20 drones to defend Tripoli from the forces of Haftar. In addition, according to news reports, Turkey has sent Syrian proxy fighters to Libya. But after the Turkish Parliament approved plans in January to send troops there, the conflict

²⁹ Frederic Wehrey, 'This War Is Out of Our Hands: The Internationalization of Libya's Post-2011 Conflicts from Proxies to Boots on the Ground', *New America*, 11 September 2020, 28.

³⁰ David D Kirkpatrick, 'Russian Snipers, Missiles and Warplanes Try to Tilt Libyan War', *The New York Times*, 05 November 2019.

³¹ Wehrey, 'This War Is Out of Our Hands', 29–30.

³² Daren Butler and Tuvan Gumrukcu, 'Turkey signs maritime boundaries deal with Libya amid exploration row', *Reuters*, 28 November 2019.

³³ 'After the maritime agreement ... Turkey announces a new step in military cooperation with Libya', *Teller Report*, 15 December 2019.

³⁴ Ceyda Caglayan, 'Turkey aims to sign deal with Libya over Gaddafi-era compensation', *Reuters*, 10 January 2020.

escalated even further, and has become a chaotic proxy war between multiple powers for control of the oil-rich country.³⁵

The proxy forces dispatched by Turkey to Libya in December 2019 comprised an initial part of a few thousand fighters drawn from Turkish-backed Syrian militias, some of whose members had fought in Syria's civil war. These Syrian fighters were delivered by civilian aircraft and ships into Tripoli and Misrata. Many of them were ethnic Turkmen with close familial ties to Turkey, and in return for their service, they were offered huge salaries and the promise of Turkish citizenship. The additional Turkish military support among others consisted of more Bayraktar TB2 drones, sophisticated air defence systems and electronic warfare equipment. Turkey's layered air defence systems effectively negated Haftar's air advantage over Tripoli and Misrata, thus GNA forces around the capital were suddenly afforded greater mobility. A foreign military intervention on this scale can have a decisive effect on the course of the battlefield – as we have seen this already at the fall of Gaddafi –, thus Turkey eventually managed to turn the battle for Tripoli.³⁶ However, while the Syrians meant much help, they also stirred some controversy, since some GNA commanders resented the deployment of foreign infantry, arguing that what was really needed was advanced weapons and equipment, not foreign manpower. Still, by creating a new balance between the opposing forces on the frontline, the Turkish intervention with the deployment of Syrian fighters enabled a push by Moscow and Ankara to try and mediate an end to the conflict.³⁷

Finally, on January 12, Vladimir Putin, in coordination with Erdoğan, hosted a summit in Moscow that both the GNA prime minister al-Sarraj and Haftar attended, resulting in a commitment to a truce. But only al-Sarraj signed the agreement, because Haftar later walked out of the meeting. Partially motivated by the Moscow summit and the opportunity opened by Haftar's walkout, the European countries finally were able to mobilise and reach a consensus on talks of their own. Right after the Moscow summit, another international conference convened on January 18, hosted by German Chancellor Angela Merkel. In the final communique of the participants, the international parties committed to enforcing the arms embargo and working toward a truce. However, aerial and maritime arms shipments into Libya resumed almost as soon as the peace conference ended. The first months of 2020 thus went by with the build-up and regrouping of the opposing forces, supported by their foreign patrons. After the Berlin conference, the UAE tried to compensate for the Turkish intervention by flying in equipment in heavy aircraft to eastern Libya to beef up Haftar's forces.³⁸ Turkey also sent more advisers and officers, self-propelled artillery, radars, tanks and even naval frigates with helicopters, which would eventually be used in a counterattack on Haftar's forces.³⁹

³⁵ Carlotta Gall, 'Turkey, Flexing Its Muscles, Will Send Troops to Libya', *The New York Times*, 02 January 2020.

³⁶ Ben Fishman and Conor Hiney, 'What Turned the Battle for Tripoli?', Policy Analysis/Policy Watch 3314, *The Washington Institute*, 06 May 2020.

³⁷ Wehrey, 'This War Is Out of Our Hands', 31–32.

³⁸ Jason Burke and Patrick Wintour, 'Suspected military supplies pour into Libya as UN flounders', *The Guardian*, 11 March 2020.

³⁹ Metin Gurcan, 'Battle for air supremacy heats up in Libya despite COVID-19 outbreak', *Al-Monitor*, 06 April 2020.

In mid-April 2020, Libya’s internationally recognised government announced that its troops have seized control of three strategic coastal cities located between the capital, Tripoli and the Tunisian border after finally expelling Haftar’s forces. Meanwhile, the UAE and the LNA forces stepped up on the attack against Tripoli and sought to counterbalance Erdoğan’s Syrian deployment with sending their own foreign mercenaries. Abu Dhabi and the Wagner Group had already channelled Chadian and Sudanese fighters into the front, but later militiamen have been flown into Libya even by the Damascus-based Cham Wings Airlines to support Haftar’s forces. According to a UN report, about 800 to 1,200 mercenaries from the Russian Wagner Group have been actively operating in Libya since 2018, including at least 39 Russian snipers on the front lines, while as many as 2,000 Syrians have likely been flown into Libya by Cham Wings Airlines to back Haftar.⁴⁰

Thanks to the deployment of Turkish troops and air support, the GNA eventually was able to reclaim several towns in western Libya, while Haftar’s forces have been forced to retreat to around Tripoli and Tarhouna. But the sudden and huge increase of the level of Turkish and Russian involvement after December 2019 has quickly led to Ankara and Moscow gaining influence on the ground, while hindering European interests and potentially sidelining the West out of any peace settlement.⁴¹

Table 1: Russian and Turkish military intervention in the Libyan civil war

External intervener	Russia	Turkey
Side	Haftar’s LNA forces	UN-backed GNA
Political Agenda	Gain regional influence Access to natural resources	Maintain economic interests Secure the 2019 maritime and security agreement Expand regional influence Block Emirati expansion and Russian influence
Force	Wagner Group (2,500) and other foreign mercenary forces (3,800 Syrian fighters) MiG-29, SU-24 and SU-35 fighter jets, arms, equipment and other supplies Parallel currency	Bayraktar TB2 drones, Hawk missiles and air defence systems Jamming gear Mercenary forces Training and other military resources
Stakes	Economic gains Access to southern Mediterranean Prestige and great power status	Economic gains Maritime border disputes Access and regional influence

Source: Megerisi, ‘Geostrategic Dimensions’, 6.

Breaking the counter-interventional cycles

In the summer of 2020, the fighting concentrated to the areas around Jufra and the city of Sirte, while Russia continued to ship arms and sent secretly repainted combat aircraft from Syria to eastern Libya. Russia also repositioned Wagner Group fighters around Sirte,

⁴⁰ David Wainer, ‘Russian Mercenaries Act as ‘Force Multiplier’ in Libya, UN Says’, *Bloomberg*, 05 May 2020.

⁴¹ Megerisi, ‘Geostrategic Dimensions’, 6.

strategic air bases across Fezzan and key oil fields. In June, Egyptian president Sisi warned that Sirte was a redline for him and he even threatened a military intervention to halt Turkey's advance to the east. But despite Sisi's warning, Turkey has been repositioning its military assets and weapons, preparing for an assault on Sirte. Meanwhile on the diplomatic front, the United States finally started pressing for a demilitarisation zone in Sirte as a means of securing a return to a political process. In this effort, Germany, the United Kingdom and the UN also took part. The U.S. ambassador to Libya engaged in shuttle talks with Ankara and Cairo, resulting in their support to a ceasefire agreement announced on August 21, 2020 by GNA Prime Minister al-Sarraj and the speaker of the eastern House of Representatives (HoR), Aguila Saleh.⁴²

In September, Abdallah al-Thani, the prime minister of the interim government in eastern Libya, submitted the resignation of his government to Aguila Saleh amid street protests that erupted across the divided country over dire living conditions. According to the UN Support Mission in Libya the protests across the country were 'motivated by deep-seated frustrations about sustained poor living conditions, shortages of electricity and water, rampant corruption, misgovernance, and a lack of service provision'. The situation clearly indicated the urgent need to lift the oil blockade imposed by tribes loyal to Haftar in the east and the return to the political process to end Libya's years long conflict.⁴³ A few days later even Prime Minister Fayez Al-Sarraj, head of the Tripoli-based GNA, announced his intention to step down by the end of October, but weeks later he reversed his decision. On 23 October, the rival forces finally agreed on a permanent nationwide ceasefire including the departure of all foreign fighters and mercenaries from the country. This progress on the diplomatic front meant that the focus now shifted to whether the foreign actors in Libya will end supporting the warring sides and withdraw their troops. Turkey has sent approximately 4,000 Syrian mercenaries to support the UN-backed GNA, while fighters from the Russian Wagner Group have supported Haftar, and a steady flow of weaponry has been sent by the UAE in a clear breach of the UN arms embargo.⁴⁴ As a part of the preliminary ceasefire agreement, Libya's rival leaders kicked off a UN-brokered prisoner exchange in December 2020, while Turkey's Defense Minister Hulusi Akar, the military chief of staff Yasar Guler and other military commanders visited Tripoli where they were meeting with their allies in the UN-backed GNA.⁴⁵ One day later senior Egyptian security officials have also visited Tripoli for the first time in years and held talks with officials from the GNA.⁴⁶

⁴² Declan Walsh, 'Libyan Rivals Call for Peace Talks. It May Be Wishful Thinking', *The New York Times*, 21 August 2020.

⁴³ Samy Magdy, 'Officials say east Libya government resigns amid protests', *The Washington Post*, 13 September 2020.

⁴⁴ Patrick Wintour, 'Libya's rival forces sign permanent ceasefire at UN-sponsored talks', *The Guardian*, 23 October 2020.

⁴⁵ Samy Magdy, 'UN: Libya's rivals swap prisoners, part of cease-fire deal', *AP News*, 26 December 2020.

⁴⁶ Al Jazeera, 'Egyptian delegation visits Libyan capital for talks with GNA', 27 December 2020.

Conclusion

Summarising the history of Libya in recent years, we can say that the country virtually has sunk into chaos since the overthrow of Gaddafi and become divided between the internationally recognised government in Tripoli on the west, and a parallel administration on the east, which got allied to General Haftar. In a few years, Haftar has turned into a major player in Libya, thanks mainly to the backing of Egypt and the UAE which see him as a bulwark against Islamists. The Libyan civil war has intensified particularly in April 2019, after Haftar's Libyan National Army launched an offensive to capture Tripoli to oust the UN-supported GNA. But Haftar's military advances got halted due to Turkey's military intervention, which led to a return to the negotiating table.

By the efforts of the UN, an agreement on a political solution to the crisis was reached. However, one of the fundamental challenges facing any effort to reach a political solution in Libya is the fragmentation of national authority and the deep internal divisions. It must also be noted that the Libyan conflict is constantly changing, which makes it difficult to be always aware of all the recent developments on the ground. The alliances among the actors are constantly fluctuating, while foreign interference is also a determining factor. External actors ultimately lack the trust of the Libyan society due to the fact that they are foreign. However, while Libyans view the international community with suspicion, they still appreciate the UN's efforts to reach a political solution and believe that perhaps it is the only organisation capable of solving the conflict.⁴⁷

So, though the agreement on a permanent ceasefire and the latest developments in December 2020 are good signs, still, the peace process remains fraught with some major pitfalls. Besides the internal dynamics, the prospect for a durable peace is still offset by the calculations of the foreign actors and especially of the direct interveners, who continue to try to secure their political and economic interests for the long run. Maybe one of the most significant challenges of the peace process is the fact that the signatories have a limited span of control over armed and political actors on the ground.⁴⁸ But we should also bear in mind that external interventions usually prolong the given conflict, while any increase in the level of its internationalisation threatens the future of Libya and its territorial integrity.⁴⁹

References

'After the maritime agreement ... Turkey announces a new step in military cooperation with Libya'. *Teller Report*, 15 December 2019. Online: www.tellerreport.com/news/2019-12-15—after-the-maritime-agreement—turkey-announces-a-new-step-in-military-cooperation-with-libya-.B1J2BOQCH.html

⁴⁷ José S Vericat and Mosadek Hobrara, 'From the Ground Up: UN Support to Local Mediation in Libya', *International Peace Institute*, 01 June 2018, 18–20.

⁴⁸ Wehrey, 'This War Is Out of Our Hands', 37.

⁴⁹ 'Turkey's Growing Role in Libya', 4.

- Al Jazeera, 'Egyptian delegation visits Libyan capital for talks with GNA', 27 December 2020. Online: www.aljazeera.com/news/2020/12/27/egyptian-delegation-visits-libyan-capital-for-talks-with-gna
- Al Jazeera, 'Haftar: Libya's UN-backed government's mandate obsolete', 18 December 2017. Online: www.aljazeera.com/news/2017/12/18/haftar-libyas-un-backed-governments-mandate-obsolete
- Al Jazeera, 'Libya, Turkey sign deals on security and maritime jurisdictions', 28 November 2019. Online: www.aljazeera.com/news/2019/11/28/libya-turkey-sign-deals-on-security-and-maritime-jurisdictions
- Al Jazeera, 'Libya's Haftar vows to fight until Tripoli 'militias' defeated', 26 May 2019. Online: www.aljazeera.com/news/2019/5/26/libyas-haftar-vows-to-fight-until-tripoli-militias-defeated
- Al Jazeera, 'Timeline: Haftar's months-long offensive to seize Tripoli', 19 February 2020. Online: www.aljazeera.com/news/2020/2/19/timeline-haftars-months-long-offensive-to-seize-tripoli
- Al Jazeera, 'Trump praises Haftar in apparent reversal of US policy on Libya', 20 April 2019. Online: www.aljazeera.com/news/2019/4/20/trump-praises-haftar-in-apparent-reversal-of-us-policy-on-libya
- Al Jazeera, 'UN envoy: 'Libya a textbook example of foreign intervention'', 23 May 2019. Online: www.aljazeera.com/news/2019/5/23/un-envoy-libya-a-textbook-example-of-foreign-intervention
- Allahoum, Ramy, 'Libya's war: Who is supporting whom'. *Al Jazeera*, 09 January 2020. Online: www.aljazeera.com/news/2020/1/9/libyas-war-who-is-supporting-whom
- Anderson, Jon Lee, 'The Unravelling'. *The New Yorker*, 16 February 2015. Online: www.newyorker.com/magazine/2015/02/23/unravelling
- BBC, 'Khalifa Haftar: The Libyan general with big ambitions', 08 April 2019. Online: www.bbc.com/news/world-africa-27492354
- Burke, Jason and Patrick Wintour, 'Suspected military supplies pour into Libya as UN flounders'. *The Guardian*, 11 March 2020. Online: www.theguardian.com/world/2020/mar/11/suspected-military-supplies-libya-un-cargo
- Butler, Daren and Tuvan Gumrukcu, 'Turkey signs maritime boundaries deal with Libya amid exploration row'. *Reuters*, 28 November 2019. Online: www.reuters.com/article/us-turkey-libya/turkey-signs-maritime-boundaries-deal-with-libyaamid-exploration-row-idUSKBN1Y213I
- Caglayan, Ceyda, 'Turkey aims to sign deal with Libya over Gaddafi-era compensation'. *Reuters*, 10 January 2020. Online: www.reuters.com/article/us-libya-security-turkey/turkey-aims-to-sign-deal-with-libya-over-gaddafi-era-compensation-idUSKBN1Z913A
- Cumming-Bruce, Nick and Declan Walsh, 'Libya Cease-Fire Raises Hopes for Full Peace Deal'. *The New York Times*, 23 October 2020. Online: www.nytimes.com/2020/10/23/world/middleeast/libya-ceasefire.html
- 'Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011)'. *United Nations Security Council*, S/2019/914, 09 December 2019. Online: www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_914.pdf

- Fishman, Ben and Conor Hiney, 'What Turned the Battle for Tripoli?' Policy Analysis/Policy Watch 3314, *The Washington Institute*, 06 May 2020. Online: www.washingtoninstitute.org/policy-analysis/what-turned-battle-tripoli
- Gall, Carlotta, 'Turkey, Flexing Its Muscles, Will Send Troops to Libya'. *The New York Times*, 02 January 2020. Online: www.nytimes.com/2020/01/02/world/europe/erdogan-turkey-libya.html
- Gurcan, Metin, 'Battle for air supremacy heats up in Libya despite COVID-19 outbreak'. *Al-Monitor*, 06 April 2020. Online: www.al-monitor.com/pulse/originals/2020/04/turkey-libya-air-supremacy-heats-up-despite-amid-coronavirus.html
- 'Joint Statement on U.S.–Libya Security Dialogue'. *U.S. Department of State*, 14 November 2019. Online: www.state.gov/joint-statement-on-u-s-libya-security-dialogue/
- Kirkpatrick, David D, 'Russian Snipers, Missiles and Warplanes Try to Tilt Libyan War'. *The New York Times*, 05 November 2019. Online: www.nytimes.com/2019/11/05/world/middleeast/russia-libya-mercenaries.html
- Magdy, Samy, 'Officials say east Libya government resigns amid protests'. *The Washington Post*, 13 September 2020. Online: www.washingtonpost.com/world/africa/officials-say-east-libya-government-resigns-amid-protests/2020/09/13/f592e25c-f605-11ea-85f7-5941188a98cd_story.html
- Magdy, Samy, 'UN: Libya's rivals swap prisoners, part of cease-fire deal'. *AP News*, 26 December 2020. Online: <https://apnews.com/article/africa-geneva-libya-tripoli-prisoner-exchange-4071811c190fcabc6c996f10af8baab2>
- Malsin, Jared and Summer Said, 'Saudi Arabia Promised Support to Libyan Warlord in Push to Seize Tripoli'. *The Wall Street Journal*, 12 April 2019. Online: www.wsj.com/articles/saudi-arabia-promised-support-to-libyan-warlord-in-push-to-seize-tripoli-11555077600
- Megerisi, Tark, 'Geostrategic Dimensions of Libya's Civil War'. *Africa Security Brief* No 37, May 2020. Online: www.jstor.org/stable/resrep24408
- Polat, Ferhat, 'The trajectory of Turkey–Libya relations'. *TRT World*, 30 August 2019. Online: www.trtworld.com/opinion/the-trajectory-of-turkey-libya-relations-29413
- Reuters, 'Forces loyal to Libya's U.N.-backed government receive military hardware', 18 May 2019. Online: www.reuters.com/article/us-libya-war-arms/forces-loyal-to-libyas-un-backed-government-receive-military-hardware-idUSKCN1SOOKD
- Tanchum, Michael, 'A dangerous policy of Turkish containment in the Eastern Mediterranean'. *The Jerusalem Post*, 10 July 2019. www.jpost.com/Opinion/A-dangerous-policy-of-Turkish-containment-in-the-Eastern-Mediterranean-595269
- The Guardian, 'UN-supported Libya government and rival authority call ceasefire', 21 August 2020. Online: www.theguardian.com/world/2020/aug/21/rival-libya-parliament-backs-un-supported-government-ceasefire
- 'Turkey's Growing Role in Libya: Motives, Background and Responses', *Arab Center for Research & Policy Studies*, 15 January 2020. Online: www.jstor.org/stable/resrep24490
- Vericat, José S and Mosadek Hobrara, 'From the Ground Up: UN Support to Local Mediation in Libya'. *International Peace Institute*, 01 June 2018. Online: www.jstor.org/stable/resrep19632.9

- Wainer, David, 'Russian Mercenaries Act as 'Force Multiplier' in Libya, UN Says'. *Bloomberg*, 05 May 2020. Online: www.bloomberg.com/news/articles/2020-05-05/russian-mercenaries-act-as-force-multiplier-in-libya-un-says
- Walsh, Declan, 'Libyan Rivals Call for Peace Talks. It May Be Wishful Thinking'. *The New York Times*, 21 August 2020. Online: www.nytimes.com/2020/08/21/world/middleeast/libya-ceasefire.html
- Wehrey, Frederic, 'This War Is Out of Our Hands: The Internationalization of Libya's Post-2011 Conflicts from Proxies to Boots on the Ground'. *New America*, 11 September 2020. Online: www.jstor.org/stable/resrep26366
- Wintour, Patrick, 'Libya's rival forces sign permanent ceasefire at UN-sponsored talks'. *The Guardian*, 23 October 2020. Online: www.theguardian.com/world/2020/oct/23/libya-rival-forces-sign-permanent-ceasefire-at-un-sponsored-talks
- Yaakoubi, Aziz El, 'Libyan factions sign U.N. deal to form unity government'. *Reuters*, 17 December 2015. Online: www.reuters.com/article/us-libya-security-idUSKBN0U00WP20151217

The Remarkable 10th Anniversary of Stuxnet¹

Analytical Summary of the SolarStorm Cyber Espionage Campaign

Gábor SELJÁN²

It has been ten years since Stuxnet, a highly sophisticated malware that was originally aimed at Iran's nuclear facilities, was uncovered in 2010. Stuxnet is considered to be the first cyber weapon, used by a nation state threat actor in a politically motivated cyberattack. It has significantly changed the cybersecurity landscape, since it was the first publicly known malware that could cause physical damage to real processes or equipment. Its complexity and level of sophistication, due to the exploitation of four different zero-day vulnerabilities in Windows and the usage of two stolen certificates, has triggered a paradigm shift in the cybersecurity industry. The recently uncovered cyber espionage campaign known as SolarStorm is a worthy anniversary celebration for Stuxnet. Especially because now the tables have turned. This campaign targeted the United States Government and its interests with a highly sophisticated supply chain attack through the exploitation of the SolarWinds Orion Platform used by thousands of public and private sector customers for infrastructure monitoring and management. In this article, I attempt to summarise the key points about the malware deployed in the SolarStorm campaign that can be drawn from reports available at the time of the writing.

Keywords: backdoor, cybersecurity, cyber warfare, malware, supply chain attack

Introduction

2020 has brought many challenges and changes to the cybersecurity landscape. The coronavirus pandemic has forced many companies to embrace work-from-home solutions without any preparations at all. This significant transition has led to increased risks of security breaches and data thefts. However, the increasing dangers of working from home were not the only notable events regarding cybersecurity.

¹ This paper was supported by the BCE EFOP-3.6.3-VEKOP-16-2017-00007 project.

² PhD student, Corvinus University of Budapest; e-mail: gabor.seljan@stud.uni-corvinus.hu

On December 8, FireEye, one of the largest cybersecurity firms, published a blog post to notify the public of a security breach by a highly sophisticated attacker that had unauthorised access to the company's various custom-made security testing tools (for example scripts, scanners, techniques and so on) used in red-team engagements.³ This is how the investigation into the most significant cyberattack in recent memory has started. After a few days' analysis, the FireEye breach turned out to be just the tip of the iceberg. Incident responders uncovered highly sophisticated malware hiding in a worldwide used management software developed by a company called SolarWinds.

Thousands of customers turned out to be affected by a widespread software supply chain attack that compromised SolarWinds' software build process and leveraged the update mechanism of its Orion Platform to deliver a backdoor Trojan tracked as SUNBURST. Microsoft and Palo Alto refers to this still ongoing campaign of attacks connected to a suspected nation state threat actor as *Solorigate* or *SolarStorm*, respectively. Though these aliases already suggest the attack's impact on the information security industry, the purpose of this paper is to help interpret this campaign by providing both holistic and analytical summary of the sources available at the time of the writing, while focusing on key aspects of the malware, due to the scale and complexity of the campaign.

The sum of all fears

“You may take the most gallant sailor, the most intrepid airman, or the most audacious soldier, put them at a table together — what do you get? The sum of their fears.”

Winston Churchill

Trusting trust

Back in 1984, in his Turing Award Lecture, Ken Thompson brought forth one of the most significant security challenges that the information technology industry faces: *trust*. Thompson described how easily an attacker could change a compiler binary to produce malicious versions of some programs, including the said compiler itself. This chicken or egg problem demonstrates that there is no truly trustworthy solution to verify the originality and the integrity of software.

You can't trust code that you did not totally create yourself.... No amount of source-level verification or scrutiny will protect you from using untrusted code.... As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.⁴

³ FireEye, 'Unauthorized Access of FireEye Red Team Tools', 08 December 2020.

⁴ Ken Thompson, 'Reflections on Trusting Trust', *Communications of the ACM* 27, no 8 (1984), 761–763.

This problem affects the setup and update mechanisms of our information systems being used today, because most application installations and system updates are performed with very high privileges. We simply cannot implement such complex systems by ourselves, hence we completely trust the vendor of the operating system running on our machine, because vendors have practically unlimited power over the device the operating system runs on. In most cases, Windows Updates are automatically installed in the background in the context of the SYSTEM user, while on Linux systems packages are usually manually applied with root privileges, though some distributions install security patches automatically. Security tools and appliances also typically run with high privileges and have access to sensitive assets. This trust relationship between customers and vendors makes the supply chain an extremely valuable target for threat actors.

Software supply chain attacks seek to damage government agencies and economic operators by targeting elements at any levels in their supply chain, including sub-contractors, integrators and so on. The attack could occur at any location in the supply chain, including development tools or business processes. For example, by inserting malicious software components during early phases of the software development lifecycle, adversaries could gain control of the systems using the malicious software for later remote exploitation. In his technical report submitted to MITRE in 2013, John F Miller gathered a wide range of supply chain attack information and provided a comprehensive view of supply chain attacks of malicious insertion across the full acquisition lifecycle.⁵

While these types of attacks have been around now for decades, they have started to become a hot topic in the security world, as the number of attacks, their sophistication and impact increased in the past few years. In his talk, in 2018 at the *BlueHat* conference, Elia Florio described 2017 as the year when the growing trend of such attacks became concerning.⁶ Palo Alto Networks also laid out notable software supply-chain attacks in their professional blog, highlighting incidents involving Apple's *Xcode* software and *Transmission*, a popular open source BitTorrent client, and predicting an increased focus on attacking trusted developers.⁷

Among the several reported breaches, for example, *Cisco* revealed that the *CCleaner* installer distributed over a month's period contained a malicious payload.⁸ Even today, it is still a very popular application used by many administrators to perform routine system maintenance. Reports at that time suggested that the malicious version of the application had been installed 2.27 million times until *Cisco* discovered the rouge app, hence the potential impact of this incident was severe.⁹

It is also among the most notable incidents of recent time, when Mossad, the Israeli secret service alerted the United States of America (USA) in 2015, after discovering attackers searching computers worldwide for documents with information regarding American

⁵ John F Miller, 'Supply Chain Attack Framework and Attack Patterns', *MITRE*, December 2013.

⁶ Elia Florio, 'Software Supply Chain Attacks in 2018', *Microsoft*, 30 November 2018.

⁷ Ryan Olson, 'The Era of Software Supply-Chain Attacks Has Begun', *Palo Alto Networks*, 18 December 2017.

⁸ Edmund Brumaghin, Ross Gibb, Warren Mercer, Matthew Molyett and Craig Williams, 'CCleanup: A Vast Number of Machines at Risk', *Cisco Talos Intelligence Group*, 18 September 2017.

⁹ Andy Greenberg, 'Software Has a Serious Supply-Chain Security Problem', *Wired*, 18 September 2017.

intelligence programs. This incident became infamous, because authorities confirmed that Russian attackers were able to steal confidential documents from the National Security Agency (NSA), through an employee who had improperly stored them on his personal computer running Kaspersky Lab's anti-virus software, which the attackers used as their very own search engine to conduct cyber espionage.¹⁰

There was another supply chain related security breach, with the probable involvement of the NSA, which have made the headlines in 2015. The National Institute of Standards and Technology (NIST) published an encryption algorithm in 2006 as a government standard at the NSA's request, despite the concerns of independent cryptography experts, suggesting that the proposed algorithm likely contained a backdoor that could be used to decrypt data. In 2008, the algorithm was secretly added to several Juniper products at the request of a customer, whom Juniper refused to identify.

In 2015, the company publicly revealed that its systems have been hacked in 2012, likely by a foreign government, and the intruder made a small code change of the said algorithm, that could be exploited to decrypt sensitive data.¹¹ Several United States government officials still seek answers to many questions regarding Juniper's internal investigation into the origin of the suspected NSA backdoor mechanism. In their open letter sent to Juniper, they have asked the vendor to publish the results of their investigation: 'Juniper's experiences can provide a valuable case study about the dangers of backdoors, as well as the apparent ease with which government backdoors can be covertly subverted by a sophisticated actor.'¹²

Basic cyber hygiene

History also shows that SolarWinds had struggles to get basic security hygiene implemented. As Bloomberg reported, a former security adviser of SolarWinds had warned the company's management of security risks in 2017. A former software engineer of the company also shared the view that a major breach is inevitable at SolarWinds, if they do not commit to security.¹³ Their opinion seems to be justified by the fact that the company was also alerted in 2017, by an independent security researcher, because their update server was accessible with an easily guessable default password *solarwinds123*.

Further reinforces the negative image that the malicious binaries were still available for download days after the incident have been publicly disclosed and security updates have been published.¹⁴ The firm also advised customers in a support page to exclude files, directories and ports from antivirus protection to run SolarWinds products more

¹⁰ Nicole Perlroth and Scott Shane, 'How Israel Caught Russian Hackers Scouring the World for U.S. Secrets', *The New York Times*, 10 October 2017.

¹¹ Kim Zetter, 'Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA', *Wired*, 22 December 2015.

¹² Catalin Cimpanu, 'Congress asks Juniper for the results of its 2015 NSA backdoor investigation', *ZDNet*, 10 June 2020.

¹³ Ryan Gallagher, 'SolarWinds Adviser Warned of Lax Security Years Before Hack', *Bloomberg*, 21 December 2020.

¹⁴ Raphael Satter, Christopher Bing, Joseph Menn, 'Hackers used SolarWinds' dominance against it in sprawling spy campaign', *Reuters*, 16 December 2020.

efficiently. This is a quite common practice by vendors to avoid conflicts with endpoint protection software and often implemented using broad exclusion rules.¹⁵

Zero Day Initiative (ZDI) published details of some recently patched vulnerabilities in the Orion Platform, including a remote code execution vulnerability known as CVE-2020-14005 and a privilege escalation vulnerability through an SQL injection bug identified as CVE-2020-27869. These are low complexity, easily identifiable security flaws that might not seem to be severe by themselves, as they are only exploitable after user authentication. However, combining these vulnerabilities with the previously mentioned authentication bypass vulnerability tracked as CVE-2020-10148, could allow an unauthenticated remote attacker to take full control of the affected system.¹⁶

Weapons of mass espionage

SUNBURST

Initial reports suggested, but during the writing of this paper the vendor also confirmed, that the actors behind the SUNBURST malware have tested their methodology as early as September 2019, without performing any other malicious actions, to ensure that their modifications to the SolarWinds Orion code base would arrive to customers undetected. As a highly organised and disciplined attacker, the threat actor left a very narrow window of time between the compilation and the deployment of the compromised code base and later also removed the malware from the build environment. In their filing with the Securities and Exchange Commission (SEC) on December 21, 2020, SolarWinds confirmed that the malicious code appears to have been inserted during the build process and was not found in the source code of the Orion Platform products.¹⁷

According to Charles Carmakal, chief technology officer at Mandiant, FireEye's incident response arm, their security team received an alert, after a new unknown device has been registered with the company's multi-factor authentication system. This event prompted FireEye to investigate the situation. As FireEye was working to determine how the intruders have obtained the employee's credentials to register their device, they uncovered the SolarWinds breach into their network. The attackers presumably obtained the employee's credentials once they were already inside FireEye's network.¹⁸

Researchers recovered multiple malware samples that deliver different payloads, including novel memory-only droppers known as TEARDROP and RAINDROP. In one analysed case, the threat actor used TEARDROP to deploy BEACON, a payload included with Cobalt Strike, which is a well-known penetration testing tool based on the Metasploit Framework. The malware runs in-memory, but it registers a Windows service that calls the

¹⁵ Tara Seals, 'The SolarWinds Perfect Storm: Default Password, Access Sales and More', *Threatpost*, 16 December 2020.

¹⁶ Sivathmican Sivakumaran, 'Three Bugs in Orion's Belt: Chaining Multiple bugs for Unauthenticated RCE in the SolarWinds Orion Platform', *Zero Day Initiative*, 21 January 2021.

¹⁷ Kevin B Thompson, 'FORM 8-K', *SolarWinds Corporation*, 17 December 2020.

¹⁸ Kim Zetter, 'Hackers last year conducted a dry run of SolarWinds breach', *Yahoo News*, 18 December 2020.

exported `Tk_CreateImageType` function and writes a JPEG image in the current directory. This random named image file is then decrypted, resulting in a file with a PE header that turned out to be BEACON. The attacker's choice to use a common payload seems to be odd.¹⁹

RAINDROP, uncovered by Symantec, though is a very similar loader, appears to be used for lateral movement within the victim's network. Currently available evidence suggests that it might have been delivered by other means, unlike TEARDROP, which was delivered directly by SUNBURST. It is compiled as a DLL module, which is built from a modified version of *7-Zip* source code in order to hide malicious activity.²⁰

The in-depth analysis of the malware paints a troublesome picture for the information security community and the industry. The backdoor was deployed as an update, including the digitally signed `SolarWinds.Orion.Core.BusinessLayer.dll` module, which is loaded by the legitimate `SolarWinds.BusinessLayerHost.exe` of the Orion Platform software. The trojanised update contains the backdoor that communicates to various third-party servers via HTTP protocol.

In his blog post, Tomislav Peričin, Chief Software Architect at ReversingLabs, also emphasised the level of stealth the attackers used to remain undetected as long as possible. There is a clear pattern of naming classes, members and variables appropriately to blend in with the code base, mimic the developers' coding style and naming standards. Strings are obfuscated using DEFLATE compression with Base64 encoding and 64-bit FNV-1a, a non-cryptographic hash function to hinder reverse engineering.

The malicious `OrionImprovementBusinessLayer` class and many of its methods can be found in other Orion software libraries. The attackers added a small block of code to the `InventoryManager` class to create a new thread that runs the backdoor during the legitimate background inventory checks. All these imply that the attackers were highly familiar with the code base.²¹

Several key points can be identified in the following excerpt of the code responsible for the initialisation of the backdoor. The initial analysis of this code already suggests a very specific targeting profile. Lack of evidence of second-stage payloads on the networks of many customers also suggest that instead of taking advantage of all compromised systems, the threat actor focused on some high-profile targets.

¹⁹ Check Point Research, 'SUNBURST, TEARDROP and the NetSec New Normal', *Check Point*, 22 December 2020.

²⁰ Symantec Threat Hunter Team, 'RAINDROP: New Malware Discovered in SolarWinds Investigation', *Symantec*, 18 January 2021.

²¹ Tomislav Peričin, 'SunBurst: the next level of stealth', *ReversingLabs*, 16 December 2020.

```

public static void Initialize() {
    if (GetHash(Process.GetCurrentProcess().ProcessName.ToLower()) ==
        17291806236368054941UL) { ❶
        DateTime lastWriteTime = File.GetLastWriteTime(Assembly.
            GetExecutingAssembly().Location);
        int num = new Random().Next(288, 336);
        if (DateTime.Now.CompareTo(lastWriteTime.AddHours((double)num)) >= 0) { ❷
            instance = new NamedPipeServerStream(appId);
            ConfigManager.ReadReportStatus(out status);
            if (status!= ReportStatus.Truncate) {
                DelayMin(0, 0);
                domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
                if (!string.IsNullOrEmpty(domain4) &&!IsNullOrEmpty(domain4)) { ❸
                    DelayMin(0, 0);
                    if (GetOrCreateUserID(out userId)) { ❹
                        DelayMin(0, 0);
                        ConfigManager.ReadServiceStatus(false);
                        Update(); ❺
                        instance.Close();
                    }
                }
            }
        }
    }
}

```

On execution of the `Initialize()` method, the malware performs several checks to verify that the infected system is among the target machines. ❶ It verifies the name of the process using a hash, ❷ the write time of the assembly and ❸ checks that the machine is domain joined. The malware then ❹ generates a unique identifier for the victim machine and ❺ invokes the method `Update()` which is the core event loop for periodic beaconing to the command and control (C&C) server. The patience and operational security demonstrated by this threat actor allowed the malware to stay hidden and operate for a long period of time.

After an initial dormant period of 12–14 days (depending on a random offset), it attempts to resolve a subdomain of `avsvmcloud[.]com` to get in contact with its designated C&C server, from which it retrieves and executes various built-in commands that, among other things, allow internal reconnaissance, persistence and data exfiltration. In order to evade detection, the malware masquerades its communication as legitimate network traffic, stores information within original configuration files to blend in with usual application activity and uses extensive blocklists to avoid forensic and anti-virus tools.

Subdomains are constructed by a Domain Generation Algorithm (DGA) to vary DNS requests and to control the behaviour of the malware on specific targets based on their unique identifier.²² On December 15, 2020, Microsoft intervened in cooperation with industry partners, and seized the domain name `avsvmcloud[.]com` used for the campaign. By sinkholing the C&C communication with the compromised systems, they effectively

²² FireEye, ‘Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor’, 13 December 2020.

rendered this malware inoperable.²³ Anyway, the shutdown of one specific malware did not stop the campaign.

SUPERNOVA

As their investigation unfolded, FireEye have identified another malware named SUPERNOVA, that consists of a small persistent backdoor. Based on the technical analysis of the second malware, Wes Riley of GuidePoint Security described the operation of this backdoor in-depth in his blog post.²⁴ PaloAlto and Microsoft have also conducted their own research into SUPERNOVA and noted that – unlike in case of SUNBURST – the affected DLL module was not digitally signed, hence it was determined to be likely unrelated to the *SolarStorm* campaign and possibly used by another threat actor.²⁵

This backdoor was implemented in the form of a .NET C# web shell, as a modification to the `app_web_logoimagehandler.ashx.b6031896.dll` module that is otherwise responsible to return the user-defined logo image of the Orion web application. Traditional web shells provide a means of remote access and allow the execution of arbitrary commands on the server, by communicating with the underlying operating system via the interpreter of the scripting language being used. These tools are especially useful to exploit file inclusion vulnerabilities that allow an attacker to trick the affected application into executing malicious code.

The SUPERNOVA web shell is somewhat unconventional. The threat actor added a new `DynamicRun()` method to the `LogoImageHandler` class and appended a few new lines of argument-handling code to the beginning of the `ProcessRequest()` function to call this new method with arbitrary parameters. The new method allowed the on-the-fly compilation and in-memory execution of arbitrary .NET code supplied by the attacker via HTTP requests, leaving behind minimal forensic artifacts, as no files will be written to disk, except the temporary files used by the .NET utilities invoked during compilation of the payload. The in-memory execution of shellcode is a well-known technique used to disguise execution and bypass antivirus software. Similar web shells have been used by attackers for decades, against applications developed in common interpreted languages such as PHP or JSP. Using this technique against a system that was built in a compiled language is a novel approach.

A possible suspected entry point of the threat actor that have planted the second malware is a recently discovered authentication bypass vulnerability in the Orion Platform. This vulnerability is now known as CVE-2020-10148 and it could allow an unauthenticated remote attacker with access to the network to execute Orion API commands on the target system. As stated in the vulnerability note published by US-CERT, **1** by appending

²³ Catalin Cimpanu, 'Microsoft and industry partners seize key domain used in SolarWinds hack', *ZDNet*, 15 December 2020.

²⁴ Wes Riley, 'Supernova SolarWinds.NET Webshell Analysis', *Guide Point Security*, 17 December 2020.

²⁵ Matt Tennis, 'SUPERNOVA: A novel .NET Webshell', *Palo Alto Networks*, 17 December 2020; MSTIC, 'Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack', *Microsoft*, 18 December 2020.

specific strings like `Skipi18n` to the path of an HTTP request, the attacker could trick the Orion server to ❷ set the `SkipAuthorization` property, which may allow an API request to be processed without requiring authentication.²⁶ This property is intended for use by authentication modules that need to redirect to resources that allow anonymous connections, for example stylesheets or scripts and localisation resources.²⁷ The below is the relevant excerpt from the source code the `OnRequest()` method of the `i18nRedirector` class.

```
HttpContext context = ((HttpApplication)sender).Context;
string path = context.Request.Path;
if (path.IndexOf("Skipi18n", StringComparison.OrdinalIgnoreCase) >= 0) { ❶
    context.SkipAuthorization = true; ❷
    context.User = new NullUser();
};
```

SUNSPOT

The SUNSPOT malware is quite another piece fitting well with such sophisticated campaign like *SolarStorm*. The CrowdStrike team provided a technical analysis of this malicious tool that was deployed into SolarWinds' build environment to inject the SUNBURST backdoor into the Orion Platform without arousing any suspicion.²⁸

The malware monitored running processes on the infected machines for those involved in compilation of the Orion product and replaced one of the source files to smuggle the backdoor into the release binaries. The design suggests that the threat actor invested a lot of effort to ensure their code was properly inserted and remained undetected. According to the build timestamp found during the technical analysis of a binary sample, the malware was likely built on February 20, 2020.

The following is an excerpt of the source code of the malware that shows the method implemented for tracking build processes:

```
private static class ProcessTracker {
    private static bool SearchConfigurations() { ❶
        ManagementObjectSearcher s =
            new ManagementObjectSearcher(
                ZipHelper.Unzip(
                    "C07NSU0uUdBScCvKz1UIz8wzNooPriwuSc11KcosSy0CAA==")); ❷ // Select *
                From Win32_SystemDriver
            foreach (ManagementObject i in s.Get()) {
```

²⁶ Oliver Madison and Will Dormann, 'SolarWinds Orion API authentication bypass allows remote command execution', *CERT/CC*, 26 December 2020.

²⁷ Microsoft, 'HttpContext.SkipAuthorization Property', 31 December 2020.

²⁸ CrowdStrike Intelligence Team, 'SUNSPOT: An Implant in the Build Process', 11 January 2021.

```

ulong hash = GetHashCode(
    Path.GetFileName(
        i.Properties[ZipHelper.Unzip(
            "C0gsyfBLzE0FAA==")].Value.ToString()).ToLower()); ❷ // PathName
if (Array.IndexOf(configTimeStamps, hash) != -1) {
    return true;
}
}
return false;
}

```

The malware carries out some common steps expected from malicious code, like creating a mutex to ensure only one instance is running, creating an encrypted log file or granting itself debugging privileges to read other processes' memory. After initialisation, the malware is constantly looking for a build process using the ProcessTracker class and ❶ modifies the target source code, if the SearchConfigurations() method determines that the software being built is the Orion application.

As a fail-safe mechanism, it also checks another mutex the existence of which would instruct the malware to discretely stop and seize operation. SUNSPOT extracts the command line arguments of the build process and looks for the directory path of the Orion software, which is hard-coded in the binary in an encrypted form. ❷ String obfuscation techniques, similar to those used in SUNBURST, can be observed in the source code, leveraging DEFLATE compression and Base64 encoding. The stored malicious source code for SUNBURST is encrypted with the AES128-CBC algorithm.

To avoid errors that might raise suspicion, the threat actor also added a MD5 hash verification check to ensure compatibility with the original source. The malware replaces the source file only if both the decryption and the hash verification is successful. After the successful build of the backdoored Orion solution, the original source code is restored.

Conclusion

Ten years after Stuxnet, the cybersecurity industry have reached a new milestone. Brad Smith, president of Microsoft, wrote in his blog post that 'this attack provides a moment of reckoning' and drew attention to the need of a strong and global cybersecurity response.²⁹ Such complex and highly sophisticated attack against the United States of America by a nation state actor really represents a turning point in cybersecurity. The fact that the *SolarStorm* espionage campaign managed to infiltrate the systems of the United States government give light towards the necessity of a next paradigm shift in cybersecurity.

The Cyberspace Solarium Commission (CS) – an intergovernmental body established to develop a strategic approach to defend against significant cyberattacks – made the first

²⁹ Brad Smith, 'A moment of reckoning: the need for a strong and global cybersecurity response', *Microsoft*, 17 December 2020.

step by acknowledging that ‘the reality is that we are dangerously insecure in cyber’. The final report of the CSC offers legal and policy recommendations that signal a fundamental shift in cybersecurity policy, including a new law establishing that software vendors and hardware manufacturers are liable for damages from incidents that exploit known and unpatched vulnerabilities.³⁰

Then-president-elect Biden said in a statement, that his administration will make cybersecurity a top priority. Now the new Biden–Harris Administration has a huge amount of work to do in response to the *SolarStorm* campaign. The Trump Administration removed experienced cybersecurity professionals from their positions and eliminated several important posts altogether. Nevertheless, President Trump also made an important step to address the situation by issuing an executive order to ensure that service providers verify the identity of persons using United States Infrastructure as a Service (IaaS) and maintain records of those transactions.³¹

Attacker attribution is hard, but it is not impossible. A joint statement released by the Cyber Unified Coordination Group (UCG) on January 5, 2021, officially attributed most or all of the recently discovered cyber compromises to Russia. Kaspersky’s security researchers have also found several similarities between SUNBURST and KAZUAR, which is believed to have been used by the Russian Advanced Persistent Threat (APT) group TURLA, a sophisticated team suspected of operating out of Moscow’s FSB intelligence agency.³² The United State’s relationship with Russia was already challenging due to, among others, Moscow’s interference in the presidential election, its annexation of Crimea, its support for Syria’s Bashar al-Assad in the civil war or a second assassination attempt on Kremlin critic Alexei Navalny. This recent incident could further increase tensions with Russia.

The *SolarStorm* campaign has demonstrated that significant weaknesses in today’s cyber space – the fourth operational domain acknowledged by the NATO in 2016 – could allow determined adversaries to carry out successful targeted attacks even when lacking the economic, military and political power, by engaging in asymmetric warfare. The investigation is still ongoing and will certainly take months to conclude due to the scale of the campaign. However, seeing only the tip of the iceberg could be convincing enough to break the vicious circle of cat and mouse by changing the perspective from which we view cybersecurity today. Only by addressing the root cause can a problem be fixed.

References

Brewster, Thomas, ‘Hackers Abuse Another Adobe Zero-Day To Attack Thousands Of Web Users’. *Forbes*, 02 February 2015. Online: www.forbes.com/sites/thomasbrewster/2015/02/02/yet-another-adobe-flash-zero-day/

³⁰ Angus King and Mike Gallagher, ‘Cyberspace Solarium Commission Report’, *CSC*, 11 March 2020.

³¹ Donald J Trump, ‘Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities’, *The White House*, 19 January 2021.

³² Georgy Kucherin and Igor Kuznetsov, ‘Sunburst backdoor – code overlaps with Kazuar’, *Securelist*, 11 January 2021.

- Brumaghin, Edmund, Ross Gibb, Warren Mercer, Matthew Molyett and Craig Williams, 'CCleanup: A Vast Number of Machines at Risk'. *Cisco Talos Intelligence Group*, 18 September 2017. Online: <https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>
- Check Point Research, 'SUNBURST, TEARDROP and the NetSec New Normal'. *Check Point*, 22 December 2020. Online: <https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/>
- Cimpanu, Catalin, 'Congress asks Juniper for the results of its 2015 NSA backdoor investigation'. *ZDNet*, 10 June 2020. Online: www.zdnet.com/article/congress-asks-juniper-for-the-results-of-its-2015-nsa-backdoor-investigation/
- Cimpanu, Catalin, 'Microsoft and industry partners seize key domain used in SolarWinds hack'. *ZDNet*, 15 December 2020. Online: www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/
- CISA, 'Alert (AA20-352A)'. *Cybersecurity and Infrastructure Security Agency*, 17 December 2020. Online: <https://us-cert.cisa.gov/ncas/alerts/aa20-352a>
- CrowdStrike Intelligence Team, 'SUNSPOT: An Implant in the Build Process', 11 January 2021. Online: www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
- DHS, 'Emergency Directive 21-01'. *Department of Homeland Security*, 13 December 2020. Online: <https://cyber.dhs.gov/ed/21-01/>
- FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor', 13 December 2020. Online: www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- FireEye, 'Unauthorized Access of FireEye Red Team Tools', 08 December 2020. Online: www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html
- Florio, Elia, 'Software Supply Chain Attacks in 2018'. *Microsoft*, 30 November 2018. Online: www.youtube.com/watch?v=sMwKqSsML5E
- Gallagher, Ryan, 'SolarWinds Adviser Warned of Lax Security Years Before Hack'. *Bloomberg*, 21 December 2020. Online: www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack
- Greenberg, Andy, 'Software Has a Serious Supply-Chain Security Problem'. *Wired*, 18 September 2017. Online: www.wired.com/story/ccleaner-malware-supply-chain-software-security/
- King, Angus and Mike Gallagher, 'Cyberspace Solarium Commission Report'. *CSC*, 11 March 2020. Online: https://drive.google.com/file/d/1ryMCIL_dZ30QyJFqFkfkf10MxIXJGT4yv/view
- Lambert, John, 'Important steps for customers to protect themselves from recent nation-state cyberattacks'. *Microsoft*, 13 December 2020. Online: <https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/>
- Microsoft, 'HttpContext.SkipAuthorization Property', 31 December 2020. Online: <https://docs.microsoft.com/en-us/dotnet/api/system.web.httpcontext.skipauthorization>

- Madison, Oliver and Will Dormann, 'SolarWinds Orion API authentication bypass allows remote command execution'. *CERT/CC*, 26 December 2020. Online: <https://kb.cert.org/vuls/id/843464>
- Miller, John F, 'Supply Chain Attack Framework and Attack Patterns'. *MITRE*, December 2013. Online: www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf
- MSRC, 'Customer Guidance on Recent Nation-State Cyber Attacks'. *Microsoft*, 13 December 2020. Online: <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
- MSTIC, 'Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack'. *Microsoft*, 18 December 2020. Online: www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
- Newman, Lily H, 'Inside the Unnerving Supply Chain Attack That Corrupted CCleaner'. *Wired*, 17 April 2018. Online: www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/
- Olson, Ryan, 'The Era of Software Supply-Chain Attacks Has Begun'. *Palo Alto Networks*, 18 December 2017. Online: <https://blog.paloaltonetworks.com/2017/12/2018-predictions-recommendations-era-software-supply-chain-attacks-begun/>
- Peričin, Tomislav, 'SunBurst: the next level of stealth'. *ReversingLabs*, 16 December 2020. Online: <https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth>
- Perlroth, Nicole and Scott Shane, 'How Israel Caught Russian Hackers Scouring the World for U.S. Secrets'. *The New York Times*, 10 October 2017. Online: www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html
- Riley, Wes, 'Supernova SolarWinds.NET Webshell Analysis'. *Guide Point Security*, 17 December 2020. Online: www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/
- Satter, Raphael, Christopher Bing and Joseph Menn, 'Hackers used SolarWinds' dominance against it in sprawling spy campaign'. *Reuters*, 16 December 2020. Online: www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8
- Seals, Tara, 'The SolarWinds Perfect Storm: Default Password, Access Sales and More'. *Threatpost*, 16 December 2020. Online: <https://threatpost.com/solarwinds-default-password-access-sales/162327/>
- Sivakumaran, Sivathmican, 'Three Bugs in Orion's Belt: Chaining Multiple bugs for Unauthenticated RCE in the SolarWinds Orion Platform'. *Zero Day Initiative*, 21 January 2021. Online: www.zerodayinitiative.com/blog/2021/1/20/three-bugs-in-orions-belt-chaining-multiple-bugs-for-unauthenticated-rce-in-the-solarwinds-orion-platform
- SolarWinds, 'SolarWinds Security Advisory', 18 December 2020. Online: www.solarwinds.com/securityadvisory
- Smith, Brad, 'A moment of reckoning: the need for a strong and global cybersecurity response'. *Microsoft*, 17 December 2020. Online: <https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/>

- Symantec Threat Hunter Team, 'RAINDROP: New Malware Discovered in SolarWinds Investigation'. *Symantec*, 18 January 2021. Online: <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware>
- Tennis, Matt, 'SUPERNOVA: A novel.NET Webshell'. *Palo Alto Networks*, 17 December 2020. Online: <https://unit42.paloaltonetworks.com/solarstorm-supernova/>
- Thompson, Ken, 'Reflections on Trusting Trust'. *Communications of the ACM* 27, no 8 (1984), 761–763.
- Thompson, Kevin B, 'FORM 8-K'. *SolarWinds*, 17 December 2020. Online: <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/6dd04fe2-7d10-4632-89f1-eb8f932f6e94.pdf>
- Trump, Donald J, 'Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities'. *The White House*, 19 January 2021. Online: <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-taking-additional-steps-address-national-emergency-respect-significant-malicious-cyber-enabled-activities/>
- Zetter, Kim, 'Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA'. *Wired*, 22 December 2015. Online: www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/
- Zetter, Kim, 'Hackers last year conducted a dry run of SolarWinds breach'. *Yahoo News*, 18 December 2020. Online: <https://news.yahoo.com/hackers-last-year-conducted-a-dry-run-of-solar-winds-breach-215232815.html>

Contents

Ferenc KOCZKA: Security of Encryption Procedures and Practical Implications of Building a Quantum Computer	5
József PADÁNYI – József ONDRÉK: The Impact of the Covid Pandemic on Security and the Military: Civil-Military Cooperation in the Fight against the Covid Pandemic	23
György GULYÁS – Árpád POHL: The Role of the NATO Support and Procurement Agency in Support to Operations	37
Tibor BABOS – Gábor SINKÓ: Can Boko Haram Constitute a Threat to European Security?	53
Péter SELJÁN: Military Intervention and Changing Balance of Power in Libya	71
Gábor Selján: The Remarkable 10th Anniversary of Stuxnet	85