The Kosciuszko Institute

CYBERSEC
European Cybersecurity Forum

CYBERSECURITY COOPERATION BETWEEN POLAND AND THE UNITED KINGDOM

POLICY PAPER

AUTHORS: CIARAN MARTIN, IZABELA ALBRYCHT, MICHAŁ REKOWSKI, MACIEJ GÓRA, ŁUKASZ GAWRON

AUTHORS:

Ciaran Martin
Izabela Albrycht
Michał Rekowski[1]
Maciej Góra
Łukasz Gawron

This report was produced with the financial support of the The British Embassy in Warsaw, with full independence and intellectual freedom of its authors. The views expressed herein can in no way be taken to reflect the official opinion of The British Embassy, The Kosciuszko Institute, #CyberMadeInPoland Cluster or any other entity.

1 Views presented by author in this policy brief are his own and do not represent the official position of the European Union nor any of its institutions.

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10,
31-130 Krakow, Poland
Phone: +48 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

THE KOSCIUSZKO INSTITUTE

CYBERSECURITY COOPERATION BETWEEN POLAND AND THE UNITED KINGDOM

POLICY PAPER

INTRODUCTION – OLD ALLIANCE IN THE NEW ERA OF GLOBAL COMPETITION

The post-Cold War international order is coming to an end. A new era of global competition is emerging, with a more fragmented international system defined by weaponised economic interdependencies, radicalising geopolitical struggle and increasingly offensive use of digital technologies. For the first time in decades, we witness a formation of a global axis of authoritarian states seeking to remake the world order to their liking. These revisionist powers are already deploying their technological might to undermine democracy and crush the liberty of other nations. They actively exploit the architecture of the shared digital world to sow discord and hate, thwart human rights and civil liberties, meddle in democratic processes and compromise the security of open societies. As a consequence, cyberspace has become a highly contested environment, where state and non-state actors progressively engage in acts that endanger both international and individual security. The evolving landscape of cyber threats represents these developments, with the rise of ransomware as the most notorious threat and with state-sponsored attacks playing a more central role.

Recent weeks have attested that the geopolitical struggle between democracy and autocracy have entered a more defined phase. On 24 February 2022, the day of the unfolding of a new, full-scale aggression stage in the eight-year-long war between Ukraine and Russia, the geopolitical situation in Europe was fundamentally rewritten. In this new situation, Poland has once again found itself at the centre of global politics. As the biggest border state of the European Union and NATO, and as the first country to break the shackles of the Soviet yoke, Poland is once again becoming the country that leads the engagement between West and East. However, 30 years after the initiation of tectonic geopolitical changes in the form of the Autumn of Nations, Poland's strategic, political and economic situation is the best it has been in centuries. Poland has benefited more than any other country in Central and Eastern Europe from the systemic transformation, emerging as an economic leader in the region. Leading the movement to join the Western security architecture, it has built lasting alliances that guarantee its prosperity and security. One of the most important of those alliances, which has significantly influenced an entire generation of modern Poles, is the Polish-British strategic partnership.

Contemporary bilateral relations between Warsaw and London find their foundations in a historical relationship that was sealed during the Second World War. It was in London that the Polish government-in-exile found refuge after the Nazi-Soviet aggression on the Polish territory. Polish Army, Air Force and Navy was rebuilt in Britain and served under the British operational command, helping the Western armies achieve many successes. During the Battle of Britain, 5% of Polish pilots were responsible for 12% of all RAF victories and 303 (Polish) Fighter Squadron was recognised as the most successful of all Allied squadrons. Subsequently, 195,000 Polish soldiers fought on many western fronts.[1] But perhaps the most important – and at the same time one of the least known – Polish input in defeating the Nazis was the work of Polish cryptanalysts. Polish mathematicians Jerzy Różycki, Henryk Zygalski and Marian Rejewski began work on cracking the Enigma cipher in 1932. By 1938, thanks to Rejewski's invention of the 'cryptologic bomb', 75% of German Enigma-encrypted radio transmissions could be read. In July 1939, knowing that a German invasion of Poland was inevitable, Polish mathematicians placed their research in the hands of British and French cryptanalysts, paving the way for breaking further Enigma versions.[2] Afterwards, on the basis of the cooperation at Bletchley Park during the Second World War, a British-American cooperation was established, which later grew into the most important intelligence alliance in the world – the Five Eyes.[3]

The trust born during the war continues to this day. With nearly 800,000 Poles living and working in Britain, Polish is the second most spoken language in the UK – and English is the most spoken second language among Poles. Economic cooperation is growing rapidly, with trade turnover in 2021 of over GBP 19.5 billion and growing bilateral investments in respective markets.[4] Strong cooperation is also being established at the national security level. Given these conditions, the time has come to engage in another field of cooperation – in the technological and cybersecurity fields.

1 Mills C., Walker N., Robinson T., *Polish contribution to the UK war effort in World War Two*, *Research Briefing of House of Commons Library*, [online]: https://commonslibrary.parliament.uk/research-briefings/cdp-2019-0168/.

2 Sale T., *The Breaking of Enigma by the Polish Mathematicians*, [online]: https://www.codesandciphers.org.uk/virtualbp/poles/poles.html

3 Corera G., *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes*, [online]: https://www.bbc.com/news/uk-56284453.

4 *W relacjach z Wielką Brytanią stawiamy na inwestycje, innowacje i zielone technologie*, [online]: https://www.gov.pl/web/rozwoj-technologia/w-relacjach-z-wielka-brytania-stawiamy-na-inwestycje-innowacje-i-zielone-technologie.

1. GENERAL DIRECTION OF COOPERATION IN CYBERSPACE

Poland has a legitimate claim to be one of the UK's oldest and most important partners in computing security. The exchange of research between British, French and Polish experts in the Pyry Forest in July 1939 – the culmination of the years of work by Polish experts which was by then too dangerous to continue – proved invaluable to the subsequent cracking of Enigma in Bletchley Park. At a commemorative event in 2014 to mark its 75th anniversary, GCHQ Director Sir Iain Lobban noted that the exchange had been important enough that his predecessor, Alastair Denniston, the first head of GCHQ, had attended in person, and that both British and French cryptographic experts realised that the Poles have been considerably further ahead in their research than their western European counterparts in both the mathematics and computing science of this critically important venture.

This story is more than just an important historical anecdote. Partnership in modern cybersecurity – the successor to what would then have been known as the cipher work – depends on a mixture of trust, shared interests and capability. Without all three, cooperation is limited. None of them are built up quickly either. The fact that Poland has a long and distinguished history of expert collaboration with Britain matters.

In the light of the horrific Russian invasion of Ukraine, some parallels are being drawn between the security threats of now and those of the late 1930s. These comparisons are valid to an extent, for obvious reasons. But they have their limitations. The geopolitical threat Russia poses to the post-Cold War liberal global equilibrium is augmented by that country's significant and menacing cyber capabilities. But technology – for all its transformative benefit – is destabilising the world order in other ways beyond just giving the Kremlin a new toolkit. It has afforded less capable but still hostile powers the opportunity to acquire capabilities to menace and threaten democracies in the West to the extent that they might be unable to do in the physical world: Iran and North Korea are good examples of this, and more rogue cyber powers could be in the making. Moreover, transnational cybercrime – much, but not all, of which is based out of Russia – poses an unprecedented security and prosperity threat to citizens in countries like the UK, Poland and other allies; unprecedented because for the first time in human history it has been possible to inflict a large-scale criminal disruption, theft and harassment on another society without ever having to set foot on its or its allies' territory.

But perhaps the most important long-term strategic geopolitical change in technology is the competition for technological supremacy between the West and its free and open model of Internet-based services on the one hand, and, on the other hand, a more authoritarian model championed domestically and increasingly through exports by China. Neither Russia, nor Iran, nor North Korea have a viable separate model of technology to contest the one that has emerged in the last 30 years from the West; these powers simply misbehave and cause harm on the West's technological platforms. China is changing the basis of our understanding of technology itself.

This diverse panoply of threat requires Western powers to work together. Part of this useful collaboration can be done through formal multilateral mechanisms; the obvious example being NATO for military aspects of cyber defence and, to some extent, for cyber operations. But there is much more to cyber security than just military defence, and much more to national security collaboration than just the NATO alliance. The modern history of cybersecurity cooperation in many ways bears out the Enigma story – allies who are capable, strategically aligned, and trust each other, work together best.

That is why a renewed emphasis on the UK-Poland cyber cooperation makes sense, especially now. Poland is the largest and most strategically important of the post-Cold War allies and its interests line up naturally in many ways with those of the UK. Poland and the UK share a realisation that security requires capability and adaptation to the technological age. And cybersecurity cooperation, whilst still maturing, has been developed on the basis of trust and mutual respect.

Poland and the UK also share a broad understanding of the scope of the cybersecurity problem and what needs to be done. Core national security networks need to be protected, and a partnership between the two countries therefore requires a strong institutional framework between the countries' defence bodies. But in modern market economies, so much cyber risk is held in the private sector (often transcending national boundaries as well) that a rapid sharing of usable threat information and the sharing of best practice require an even more dynamic partnership that goes beyond traditional national security structures. Finally, the challenge posed to free and open technology by the authoritarian model championed by China requires nothing less than the West retaining (or even to some extent regaining) its confidence in the security of its own technology and, just as importantly, innovating strategically to build trustworthy, supply-chain-secured technologies of the future. This obligates countries to collaborate differently as so much of it is about economics, trade and industrial strategy rather than classic defence cooperation. But it really matters; it is only through having this reliable, secure technological base that a peaceful, secure, rules-based international system for managing the technological age can emerge.

The UK, as is clear from its Integrated Review of Security, Defence, Diplomacy and Development of March 2021 and its National Cyber Strategy adopted later that year, wants to be at the forefront of this bolstering of the international order. Both strategies explicitly acknowledge the need for strong partners across the world to deliver this vision. So far as Central and Eastern Europe is concerned, Poland should be an obvious priority for the UK in this venture.

2. CIVIL COOPERATION IN CYBERSPACE

Bilateral UK-Poland cybersecurity policy developments in recent years

Poland and the United Kingdom already initiated their cooperation in cybersecurity on the margins of the UK-Poland Treaty on Defence and Security Cooperation, signed while the British Prime Minister (PM) Theresa May was visiting Poland in December 2017. During her meeting with PM Mateusz Morawiecki, a Joint Communique was issued that declared bilateral cooperation[5] in cybersecurity in relation to the Defence Treaty, but also in the context of support for start-ups in the cyber sector. The communique was accompanied by a policy paper titled 'UK-Poland cyber co-operation commitment' that affirmed a common position of both countries on issues like applicability of international law in cyberspace and the promotion of norms and responsible behaviour to ensure the protection of human and fundamental rights in the digital domain.[6] The paper underlined both countries' commitment to free, open and peaceful cyberspace, while pointing to each state's right to develop their defensive and offensive cyber capabilities. The UK and Poland pledged to 'co-operate to deter, mitigate and attribute malicious cyber attacks by criminals, state actors and their proxies.'[7] In her speech, PM May also announced that a Polish delegation would visit the UK National Cyber Security Centre in 2018 for good-practices sharing.[8] A year later, during PM Morawiecki's visit to the UK in December 2018, both countries announced the start of joint consultations on cybersecurity in 2019, with a strengthened focus on prevention, attribution and sanctioning. Within this framework, a first round of cyber dialogue took place in 2019 in Warsaw. Another round was supposed to be held in London in 2020, but it was postponed due to the outbreak of the coronavirus pandemic. – ilt is now scheduled for the first half of 2022.

Bilateral civilian cooperation – future outlook

The renewal of the Polish-UK cyber dialogue in 2022 opens a new window of possibilities regarding the areas of engagement for both countries. Such cooperation, while managed in the civilian sector by the Polish Ministry of Foreign Affairs and the Foreign, Commonwealth and Development Office respectively, also includes several other ministries. However, it should take a more comprehensive form, guided by an all-of-government, or even all-of-society approach. The evolving character of threats in cyberspace poses a danger to the social, economic and political well-being of Polish and British societies in all areas of social live. In light of this challenge, an all-of-society exchange of good practices and expertise on issues concerning cyber resilience, cybersecurity capacity building and cybersecurity research would help to strengthen the overall resilience. Such multi-level cooperation can be built gradually, starting with the engagement of government bodies beyond the ones already active. It could include the ministries and agencies in the home affairs, justice, economy, energy, and science sectors. The collaboration should be accompanied by a growing engagement of business environment representatives and the civil society in both countries and the initiatives to create communication and frameworks to link them with each other and with the government bodies.

Concerning bilateral civilian cooperation, there are a few areas that would benefit from a rapid intensification of contacts and collaboration:

a. Operational cooperation

Given that adversarial cyber operations may be planned and carried out in order to affect targets across multiple functionalities of states and societies, a further deepening of contacts and cooperation between cyber communities in both countries should be explored, with a growing engagement of institutions like the British General Communications Headquarter (GCHQ), its subordinate National Cyber Security Centre (NCSC), and their Polish organizational counterparts at ministerial, special service and operational levels (including NASK, respective CSIRT Teams, and NCBC). Today, these institutions are the main actors responsible for both state's cybersecurity postures and capabilities and hence, they should drive the collaboration. The cross-sectoral cyber collaboration is paramount to the effective management of cyber security risks and preparation for challenges of deteriorating security environment in cyberspace. Efficient mitigation of threats in cyberspace requires tighter operational cooperation across different levels of government. Such cooperation should not limit itself and address a wide range of areas including prevention and mitigation efforts.

b. Information sharing

Access to information concerning cyber threats and cyberattacks forms a critical variable that determines the ability of states to maintain situational awareness, efficiently anticipate and mitigate risks, defend its security and sovereignty in cyberspace, but also to take informed political decisions on issues often reaching beyond the affairs of a given state. Trustworthy and verifiable information is the bedrock of all policies, including foreign policy and attribution. Both countries should work together to establish institutional frameworks for information sharing between government agencies, reaching deep across all levels, from the diplomatic leadership to cyber coordinators within different ministries, to operational bodies like cybersecurity agencies and Computer Emergency Response Teams. Specifically, for political rather than operational purposes, a functional framework should be established for information sharing that can provide detailed and reliable intelligence but will be stripped of elements that would allow others to identify the source or the techniques deployed for its gathering. It would allow for a rapid flow of key information enabling political action (such as attribution) without the need to go through multiple security air-locks that can slow down the process. This step will further the goal outlined in 2022 NCS of forming a broader international alliance that is willing and able to impose more meaningful consequences on the UK's adversaries.[9]

c. Diplomatic coordination and joint positions in multilateral governance fora

Poland and the UK are members of a number of global cyber policy organisations, including the United Nations, NATO, and OECD. Given the multitude of shared interests between the two countries and the bilateral willingness to create dialogue to build a values-driven cyber regime, these countries should support each other in facilitating processes that promote free, open, inclusive, and secure cyberspace. In particular, diplomatic efforts should aim to push the debate on norms, rules

5 *Communique: UK-Poland Inter-Governmental Consultations*, [online]: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/670518/Communique-_UK-Poland_Inter-Governmental_Consultations.pdf.

6 *UK-Poland cyber co-operation commitment*, *Policy Paper*, *Foreign*, Commonwealth & Development Office, 2017 [online]: https://www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment.

7 *Ibidem.*

8 *PM press statement in Poland: 21 December 2017*, [online]: https://www.gov.uk/government/news/pm-press-statement-in-poland-21-december-2017

9 *National Cyber Strategy 2022*, [online]: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf, p. 93.

and principles guiding responsible state behaviour in cyberspace within the UN General Assembly's First Committee, as well as support each other in the framework of UN's Global Programme on Cybercrime for the purpose of negotiating a more beneficial and comprehensive Cybercrime Treaty. Diplomatic cooperation should also be fostered in the framework of OSCE and the joint development of confidence-building measures (CBM's), especially those related to ICT threats and vulnerabilities (CBMs 1 and 16), critical infrastructure, including ICT-enabled critical infrastructure (CBMs 3 and 15) and awareness-raising (CBM 5).[10] Furthermore, the United Kingdom keeps a wide network of cyber attachés working in its diplomatic institutions across the world, and Poland has recently expanded the list of cyber attachés and intends to further develop its diplomatic capacity. Institutional consultations between both countries at the organisational level as well as the establishment of an operational dialogue between cyber attachés stationed in third countries can contribute to the UK's and Poland's diplomatic and cyber posture, also speeding up the flow of information and enhancing situational awareness of both diplomatic services.

d. Multi-sectoral coordination on cybersecurity policy issues concerning global technology providers

The pace and direction of the digital revolution that is mainly driven by market actors poses a challenge to the state's sovereignty in cyberspace. With some elements of the digital domain like certain data infrastructures, services or platforms becoming essential elements of social life or state security, big technology companies are essentially turning into gatekeepers of the digital world. And increasingly states need to deal and negotiate with these entities on equal (and sometimes unequal) terms. This also concerns cybersecurity-related issues, as some of these companies are considered to be either part of a problem or a solution. Exchange of information, good practices as well as consultations between Poland and the United Kingdom on policy and cybersecurity issues regarding these companies can positively contribute to strengthening Poland's and the UK's respective positions in the digital transformation.

e. Cooperation on education and training of cybersecurity skills

Educational cooperation should have both an academic and an institutional/operational context. Research cooperation and academic exchange programmes should be established between university students, researchers and organisations to share knowledge and experience, and to conduct joint research. The aim of this cooperation will not only be the exchange of scientific perspectives, but also the creation of a pool of cybersecurity specialists able to fill in the industry gap that already exists in both countries, allowing British cyber expertise to be exported to Central and Eastern Europe and vice versa. At the institutional level, too, not only governmental but also local, training should be introduced to expand the capacities and perspectives of public administration staff, strengthening the cyber resilience of both nations. These objectives are in line with the plans for greater international government-to-government engagement (under the auspices of the UK Cyber Security Ambassador Programme) outlined in the UK NCS as well as an increased international cooperation at the strategic political and operational-technical levels of the Polish Cyber Security Strategy.

10 *OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection*, NATO Cooperative Cyber Defence Centre of Excellence, [online]: https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/

3. MILITARY COOPERATION IN CYBERSPACE

A political and security background for the enhanced cyber defence cooperation

The status of a warfare domain, acquired by cyberspace in the NATO doctrine in 2016 alongside land, air, sea, and recently space, has advanced an understanding among the member states that defence has become an even more complex, multi-dimensional and challenging realm, with some lines between war and peace blurred due to cyber operations continuing to take place on a larger scale and magnitude under the threshold of an armed conflict.

NATO's decision has further impacted the defence forces across the Alliance and sped up the adaptation and change in regard to strategies, institutions and operations as well as bolstered the development of defensive and offensive cybersecurity capabilities along with a race for digitally and cyber savvy talent and tech innovation. Different as their pace may be, the UK and Poland have been advancing counter-cyber capabilities aimed at protecting digital infrastructure and assets from damage caused by adversaries across the entire spectrum of their military sectors. Both nations have continued the transformation to multi-domain context of military operations, which includes cyber effects. According to the Strategic Command Strategy 'states are increasingly integrating the traditional domains of land, maritime and air with the newer domains of cyberspace and space',[11] thus examining rival supply chains is necessary to 'identify weaknesses, and using a range of skills, soft and hard offensive cyber operations, to ensure ability to target those vulnerabilities.'[12] The same challenges were identified in the National Security Strategy of the Republic of Poland, particularly 'the challenges presented by the modern multi-domain operational environment, capabilities to conduct asymmetric operations.'[13]

In their respective national security strategic documents, both the UK and Poland recognize the intensifying strategic rivalry between the United States of America, the People's Republic of China and the Russian Federation 'with exercising influence of this phenomenon on the entire international system.'[14] Poland's National Security Strategy of May 2020 says that 'the neo-imperial policy of the Russian Federation authorities, pursued also by means of military force' is 'the most serious threat.' It also points out the 'multi-faceted and comprehensive actions using non-military means (including: cyber-attacks, disinformation)' undertaken by the Russian Federation to 'destabilise the structures of Western states and societies and to create divisions among Allies.' The Strategy rightly predicts the continuation of the aggressive Russian posture to undermine 'the current international order, based on international law, in order to rebuild its power and spheres of influence.' The UK's Strategic Command Strategy, published in November 2021, points out in its security environment assessment that 'Russia continues to pose the greatest nuclear, conventional military and sub-threshold threat to European security. It's a capable and unpredictable actor that is modernising its armed forces, integrating whole of state activity and demonstrating a considerable appetite for risk.' It calls for attention to its 'space and cyber and electro-magnetic domain capabilities' as well, which were probably incorporated throughout Russian incursion into Syria[15] – and are now also used

11 *The Strategic Command Strategy*, Strategic Command, [online]: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035931/The_Strategic_Command_Strategy.pdf, p. 6.
12 *Ibidem*, p.9.
13 *Strategia Bezpieczeństwa Narodowego*, [online]: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf
14 *Ibidem*, p. 7
15 *Ibidem*, p. 8.

to some extent during Russia's invasion in Ukraine. The Integrated Review of Security, Defence, Development and Foreign Policy also highlights that the UK needs to continue to adapt to a changing international environment with 'geopolitical and geo-economic shifts, such as China's increasing international assertiveness and the growing importance of the Indo-Pacific; systemic competition, including between states, and between democratic and authoritarian values and systems of government; rapid technological change.'[16] This technological challenge from Russia and China is relevant not just to Poland and the UK, but to entire NATO as it is posing new threats in cyberspace. Since 2019, NATO has been adapting to these threats by developing and implementing emerging and disruptive technologies (EDT), and underlining that the ability to carry out collective defence missions will depend on the Alliance's technological advantage over authoritarian powers which, with the help of EDT and the use of cyberspace, are increasing the effectiveness of hybrid activities and strengthening their power.[17]

The Treaty between the United Kingdom of Great Britain and Northern Ireland and the Republic of Poland on Defence and Security Cooperation signed in July 2018 acknowledged cyber-warfare and hybrid warfare as emerging security challenges and defined cyber defence, communications, electronics and information systems as the areas of cooperation. The political and security developments of the Russian war in Ukraine have now marked the right time 'to consider the progress of cooperation under this Treaty'[18] in these particular fields. Currently, while facing serious security dangers posed by the Russian Federation invading Ukraine and seeking to reshape the European geopolitics, the UK and Poland should urgently build up the security and defence collaboration further by recognising and agreeing on specific areas of cooperation to enhance the cyber defence and deterrence postures of both countries and soon introduce a strategic framework of such collaboration following the forms of cooperation specified in the Treaty.[19] In their strategic documents as well is in the Treaty, the UK and Poland perceive the cooperation with their Allies to take the shape of a bilateral and regional collaboration as a necessary step to enhance their security and 'strengthen the global and regional, rules-based security order.'[20] This approach should serve as a strong foundation for a bilateral and enhanced cooperation between Poland and the United Kingdom also in the cyber defence domain during peace and war time. Having in mind the retaliatory risks of the undergoing Russian invasion on Ukraine, the threat of conflict escalation, and several cyberattacks attributed to Russia in previous years and months, the UK and Poland should instantly structure the cyber defence cooperation around several risk scenarios emanating from cyber realm which can pose national security threats for both countries. It can be done within the provision of 'regular consultation on threats and challenges to international peace and security' regulated in the Treaty. Among the most dangerous types of cyberattacks are APTs (Advanced Persistent Threats), attacks targeting digital assets and industrial automation systems, cyber and physical attacks on the global digital infrastructure, including fibre optics, data processing centres, as well as cyberattacks on BGP (Border Gateway Protocol) and DNS (Domain Name System), which can cause severe disruptions in the functioning of the Internet. Not without significance for the escalation may also be the economic effects of Western sanctions imposed on Russia, whose hackers, especially those specialised in ransomware attacks, may want to take financial retaliation on Western companies and entities.

Although cyber operations have limited physical effects (disruption not destruction), they may, to some extent, affect the outcome of the Russian war in Ukraine and pose threats to its allies around the world. Therefore, their potential as such should not be underestimated, especially since they let preserve some degree of deniability. For this reason, NATO leaders decided at the Wales Summit in 2014 that Article 5 of the Washington Treaty would also apply if a serious cyberattack is launched on an allied country. Since the start of the Russian invasion on 24 February, NATO leaders have been repeatedly using Article 5 as a deterrence measure and a signal that it is going to be a risky game for the Kremlin, since 'the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack.'[21] It is worth noting that according to the Polish law[22], an external threat to the state, including one instigated by 'activities in cyberspace' can cause martial law to be imposed on a part or the entire territory of the state.

In the long run, in the age of advanced military solutions augmented by emerging and disruptive technologies and in the era of strategic competition and 'the strategic simultaneity,'[23] cyber bilateral cooperation will be even more important due to an observed acceleration of cyber threats. Thus, cybersecurity is going to present an even greater challenge in the military domain. According to General Sir Patrick Sanders, Commander of the UK's Strategic Command, defence must change and 'become agile, responsive and able to act in an integrated way. This means ensuring that every part of Defence can work seamlessly together with other Government departments and our allies and partners overseas. It means experimenting with new technology and becoming experts in data exploitation.'[24] The new models of innovation and application of EDTs should therefore serve as useful and important frameworks to deal with cyber threats and to improve cyber defence, deterrence, and security. The UK and Poland should consider the cooperation to be also focused on solving particular cybersecurity problem sets enhanced by EDTs, especially due to the absence of a relevant cooperation platform within the European Union.

Not only should arguments of the security threats in the turbulent present times and future challenges speak for the enhancement of cyber defence collaboration but also those from the past should do so. The shared history of ENIGMA decryption – started by the Polish scientists, fine-tuned and applied by the British scientists – is symbolic as it determined the victory of allied forces in the WWII. It gives a trustworthy framework for the two nations which share principles, norms and values to cooperate while facing strategic threats in the physical and digital realm.

16 *Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy*, p. 17.
17 I. Albrycht. W. Lorenz, *NATO Augments Its Technology Policy: Opportunities and Challenges for the Allies*, Strategic Files, PISM
18 *Treaty between The United Kingdom of Great Britain and Northern Ireland and The Republic of Poland on Defence and Security Cooperation*, Article 4, 1.b
19 There are relevant areas indicated in Article 2 of the Treaty, such as exchange of information and knowledge of security and defence policy issues, including a close dialogue on key strategic issues of mutual interest; ministerial and senior-level staff talks; engagement between military and defence institutions, including contact visits; strengthening and sustaining their capacity to deploy and operate as allies and partners in military operations, including NATO-led operations; military exercises, training and education, and the exchange of experience by the armed forces of the Parties; exchange of military and civilian personnel; creation of twin or partnership relations between military units in the armed forces of the Parties.
20 *Treaty...*, p. 3.
21 Pearson J., Landay J., *Cyberattack on NATO could trigger collective defence clause - official*, [online]:
22 *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, [online]: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20021561301/U/D20021301Lj.pdf.
23 In which numerous interconnected threats face the Alliance at the same time, according to the report *NATO 2030: United for a New Era: Analysis and Recommendations*, [online]: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.
24 *The Strategic Command Strategy*, p. 3.

A systemic and institutional background

In the context of institutional models covering military cyber dimensions, the critical competences of the UK and Poland, such as political and strategic responsibility for cyber defence as well as strategic consideration and management, are distributed among the following key governmental bodies: the Polish Ministry of National Defence (*Ministerstwo Obrony Narodowej – MON*) and the UK's Ministry of Defence (MOD) as well as their related or supervised agencies and armed forces: the National Cyberspace Security Centre – Cyber Command (*Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni*), with its newly established part – Cyberspace Defence Forces (*Wojska Obrony Cyberprzestrzeni*) in Poland and the National Cyber Force and the UK's Strategic Command which provides leadership in the cyber domain for MOD.

According to the Act on the Homeland Security (*Ustawa o obronie Ojczyzny*) signed by Polish President on 18 March 2022, the Cyberspace Defence Force have become a specialised component of the Polish Armed Forces. They are tasked with putting the full spectrum of activities in cyberspace into operation, in particular in the field of proactive and active defence of cyberspace elements and resources that are crucial from the point of view of the Polish Armed Forces.[25] CDF is responsible for conducting activities and operations in cyberspace as well as providing support for military operations conducted by the Polish Armed Forces, and operations in the allied and coalition system.[26]

Defence Digital[27] manages defensive cyber operations and maintains the overall cohesion of all information technology throughout the MOD, whilst the National Cyber Force created in 2020 as a defence-intelligence partnership, is responsible for 'operating in and through cyberspace to counter, disrupt, degrade and contest those who would do harm to the UK or its allies.'[28] NCF is part of the Ministry of Defence, the Defence Science and Technology Laboratory, the Secret Intelligence Service, and the Government Communications Headquarters.

As for the operational and cyber incident management system, in Poland, the response to attacks targeting entities subordinate to (and supervised by) the Minister of National Defence, military ICT systems and uniform services falls under the responsibility of CSIRT MON (also known as the Polish Military Computer Security Incident Response Team overseen by the Polish Ministry of National Defence and operating as a functional entity of the National Cyberspace Security Centre – Cyber Command). In the UK, the MOD Computer Emergency Response Team (MOD-CERT) is responsible for co-ordinating the MOD's response to computer security incidents.

Areas of cooperation

The military cyber cooperation between the UK and Poland should be designed in a way which will address operational challenges of the new multi-domain warfare and the growing cyber threats that may impact the security of both states, as identified above.

Information sharing

The Treaty is intended to promote 'the exchange of information and experiences regarding strategic defence and security issues.'[29] And the most important dimension of the cyber defence collaboration is indeed cyber information sharing including trends for shared situational awareness and better preparation for risk scenarios emanating from geopolitical shifts and technology advancements. At the operational level between military CSIRTs, information sharing should comprise cyber threat information and cyber intelligence which may be particularly valuable, having in mind that Poland is now being a border country in the ongoing Russian-Ukrainian war, thus exposed to the escalatory attempts and retaliatory measures below the threshold of war. Information sharing can vary in scope and develop to the extent agreed between states, possibly including the sharing of threats and vulnerability information to help manage cybersecurity risks and enhance the ability to detect, prevent, mitigate, respond to and recover from cybersecurity incidents, including tactics, techniques and procedures used by threat actors. In times of unprecedented security threats, the collaboration on upgrading capabilities among Allies, particularly to bolster their cyber defence and deterrence postures, is of great value, thus knowledge and experience exchange on cybersecurity technology and solutions is much needed. It is yet another form of information exchange which Poland and the UK can adopt as regards military cooperation.

Information and experience exchange

As described above, both states have established institutions responsible for dealing with strategic and operational military aspects of cybersecurity. However, their scale and experience vary. The Treaty recognises 'an enhanced relationship on capability development, technology, equipment, and support matters' as an important aspect of collaboration. Therefore, in the field of cyber defence, information and experience exchange can proceed with regard to cybersecurity policies, guidance, strategies and best practices, including those addressing the most pressing challenges of effective public-private partnerships, an innovation-driven defence ecosystem, a cybersecurity workforce organisation and employment system, and the overall approach to cybersecurity. It is worth noting here that the UK's National Cyber Strategy calls for 'more active and structured coordination and leadership of cyber strategy from the centre of government'[30], thus the UK's proactive approach to cybersecurity building is a good example to follow for many countries around the world in these turbulent and challenging times. Hence, the experience exchange on how to operationalise that approach should be considered by the Polish side, too. The collaboration can also target a very time-consuming process of establishing defence cyber capabilities and cybersecurity forces and can include information exchange on the development of cyber offensive capabilities as well as the conduct of cyber operations. Poland declared that it was aiming to develop those capabilities in response to the adversarial actions against their IT networks and IT/OT systems and in order to use them for defence purposes. The deteriorating security situation beyond its eastern border and the evolving cyber threats landscape require Poland to constantly advance and refine its cyber capacity. A close cooperation in this field between the Ministries of Defence in both countries can contribute to achieving this goal and help develop capabilities critical for the defence of the Polish cyberspace. At the same time, the UK is claiming to conduct cyber operations in a responsible, targeted and proportionate manner, which means the experience exchange on this matter with Poland can contribute to the sustainability of Polish cyber capacity building, the integration of best practices for conducting these operations and increasing levels

25 *Ustawa o obronie Ojczyzny*, [online]: http://orka.sejm.gov.pl/opinie9.nsf/nazwa/2052_u/$file/2052_u.pdf
26 *Ustawa o obronie Ojczyzny*, [online]: http://orka.sejm.gov.pl/opinie9.nsf/nazwa/2052_u/$file/2052_u.pdf.
27 *Defence Digital*, [online]: https://www.gov.uk/government/groups/defence-digital.
28 *National Cyber Force*, [online]: https://www.gov.uk/government/organisations/national-cyber-force.
29 *Treaty…*
30 *What does Britain's new Cyber Force mean for the future of cyber security?* [online]: https://www.dur.ac.uk/news/newsitem/?itemno=44441.

of cyber resilience in defence capabilities.[31] The UK is superior in asking itself important questions regarding the expansion of its offensive cyber operations, which create new opportunities but also give rise to key ethical and strategic dilemmas that are yet to be straightened out.[32] Such questions must be asked by other stakeholders including 'newcomers' as well. In periods when international threats escalate, like nowadays, the cooperation could go as far as conducting common operations against malicious actions to mitigate and counter cyber threats, letting each state to learn from the experiences, specific skills and analytical capabilities of others, and improving NATO's collective defences. The collaboration can also involve Rapid Response Teams of specialists, which the UK is willing to deploy also to locations overseas, in order to confront malicious cyber activity.
The UK can also share its experience on the integration of cyber operations with other 'force elements to defeat threats and enable wider defence activity.'[33]

Education and training

The most pressing challenge for cyber capacity building in both states, but also around the world, is a shortage of well-educated and savvy cybersecurity specialists. The win-win approach to this challenge lies in the cooperation between institutions responsible for cybersecurity training and education, the exchange of information and experience on best training practices, joint training within a military-to-military framework as well as the reciprocity-based exchange of experts. Education and training can serve the strategic and operational purposes of cooperation well and further strengthen mutual trust and understanding.

Forms of cooperation

Further in-depth operationalisation of the scope of cyber defence cooperation should be elaborated in the process of annual cooperation plans preparation which was established by the Treaty to set out bilateral activities to be conducted pursuant to the Treaty.[34] It should also take an official form of memorandum of understanding with complementary implementation arrangements regarding cyber defence cooperation signed by the Ministers of Defence of respective countries or Heads of NCSC-CC with National Cyber Force or Heads of CSIRT/CERTs. On a daily basis, the collaboration can take the form of working groups, discussions, study visits, conferences, training sessions and equivalent events.

31 *National Cyber Strategy 2022*, passim.
32 *What does Britain's...*, op. cit.
33 *National Cyber Strategy 2022*, p. 30.
34 *Treaty...*, Article 4, 4.

4. TECHNOLOGIES VITAL TO CYBER POWER

Novel digital technologies, particularly a group of the so-called Emerging and Disruptive Technologies (EDTs) have become the area of international rivalry where states compete to develop, master and harness technological potential to pursue their industrial, political and strategic interests. Several of such technologies, such as 5G, 6G or the Internet of Things (IoT), will significantly expand the layer of cybersecurity vulnerabilities. Others, such as Artificial Intelligence (AI) or Quantum Computing, will boost defensive and offensive cybersecurity capabilities. The intensifying race to control and exploit these technologies may result in a growing asymmetry in technological posture and cybersecurity capacities of the parties involved, with a small group of leaders assuming technological supremacy and others falling into dependency and susceptibility to external disruptions. This concern is being reflected and addressed in two key British documents: the 2021 Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy and the National Cyber Strategy 2022. The British government recognises the essential need to consciously steer the development of technologies that it considers to be central for the UK to maintain the position of Science and Tech Superpower, but also vital to the UK's Cyber Power. These include IoT, AI, Quantum, 5G & 6G, Blockchain and microelectronics. While Poland is yet to develop its comprehensive strategy concerning technologies vital to Cyber Power, there is already a broad area of cooperation that – if pursued – can help both countries advance in the technological race. Poland exhibits vast resources of highly skilled talent and innovative entrepreneurs in the technological domain that may both contribute to and benefit from a dynamic, horizontal and vertical cooperation with partners from the UK. The UK's National Cyber Strategy 2022 appreciates the positive effects of pursuing international partnerships in research, analysis, supply chains, standards and policy towards critical EDTs. Both Poland and the UK should engage in strategic cooperation – spanning academia, industry and government research agencies – to jointly advance in such high-tech sectors as the following.

Becoming cybersecurity leaders for the industry sector

The UK and Poland can concentrate their cybersecurity cooperation on technologies which will determine the shape of the Industry 4.0 and thus the future of economy, strengthening both countries' competitiveness and development of both countries in the 21st century. At least three of them can be featured: Operational Technologies, OpenRAN, and the Internet of Things together with the Industrial Internet of Things. Ensuring cybersecurity of these technologies is crucial to securing the economy of tomorrow and can become both countries' speciality. Modern technologies are the core driving force of the fourth industrial revolution because they have been effectively changing the way how modern enterprises of all sizes operate. It is mainly thanks to automation, advanced mobile internet and sensors implementation.

Operational Technologies (OT)

The physical elements of industry are controlled by the cyber and thus constitute what is now known as the cyber-physical world. More and more open and complex and integrated environments are emerging, including industrial ones, with connections to IT networks, cloud and servers, which enable remote access via, for example, frequent

updates.[35] This new incarnation of industry with IT/OT convergence – including such critical pieces of infrastructure as electricity, gas, transport, railway, water, various industry segments and processes – is therefore vulnerable to cyberattacks, incidents and interferences. The critical importance of operational technologies (OT), from which automation benefits, was highlighted in the National Cyber Strategy, which calls for 'a more proactive approach to fostering and protecting competitive advantage in the technologies critical to cyberspace,' including the ones to be developed in centres such as a national laboratory for operational technology security.[36] These technologies can address the growing threat of attacks on industrial control systems, distributed control systems and supervisory control and data acquisition systems, which can lead to material losses and serious security consequences that were not yet fully grasped in the development process of these systems. The UK is considered a world leader in research into OT security, and it can share its experience with partners as part of research programmes and through the use of facilities for running and testing these technologies. It is the same when it comes to Poland, whose structure of economy predestines it to lead in solutions for security and safety of those control systems and OT networks. Polish science and industry also has the applicable knowledge, experience and tools for cybersecurity management system for ICS and industrial automation networks to detect anomalies and cyber threats in real time, based on norms and standards, which can be deployed and scaled. Both countries and their companies can collaborate to develop advanced solutions as well as share information regarding the attacks on industrial systems to better understand their vectors, methods, and techniques. As those attacks are intentional and targeted, the techniques they utilise can therefore be repeated, while the cyber risk analysis – due to the multi-layered architecture of industrial systems – is very complex.

Internet of Things and Industrial Internet of Things

The same reasoning calls for collaboration on the security of the Internet of Things and the Industrial Internet of Things. Both technologies are rapidly transforming the economies due to a geometric increase of devices and sensors connected to the Internet, able to collect and analyse data and to deliver the new dynamic of the industrial growth and competitiveness. Closely tied to cyber-physical systems, IoT is another enabler of the Industry 4.0 with a high probability of cyberattacks, accelerated by a high quantity of devices and their insufficient security level. The complexity and the diversity of areas for IoT application make this field of collaboration very promising, since pooling knowledge and efforts can help achieve a much better level of security much faster. Cybersecurity companies gathered in the Polish Cybersecurity Cluster #CyberMadeInPoland and the Silesian IoT Cluster SINOTAIC already offer a wide range of IoT-related solutions and are ready to collaborate with their British counterparts. The UK seeks ways to build cybersecurity into IoT products, and the introduction of the Product Security and Telecommunications Infrastructure (PSTI) bill in November 2021was the first step taken to regulate this area . The bill set up new cybersecurity standards on manufacturers, importers and distributors of internet-connectable devices.

The cooperation between Poland and the UK can be arranged analogously to the NIST framework (since both countries cultivate close and cordial relationships with the United States), which promotes the collaboration of different stakeholders and supports the development and application of standards, guidelines, tools and best practices in the field of software development to enhance the cybersecurity of connected devices and the environments in which they are implemented.[37] Joint action should also target malicious malware and vulnerabilities in communication protocols which can be used as a vector for wide-spread cyberattacks exploiting IoT.

OpenRAN

The UK's National Cyber Strategy considers 5G, 6G and other emerging forms of data transmission as critical to the nation's cyber power, thus their secure development is of crucial importance to the UK. It includes 5G network solutions based on the Open RAN model – a new way of thinking about 5G architecture. OpenRAN is directly connected with a wider debate and political decisions on diversifying and securing 5G supply chains beyond traditional Big Four suppliers. That is why regulatory bodies and governments across Europe consider developing OpenRAN, since many of the European states have taken security considerations and decisions related to identifying trustworthy 5G network suppliers , and increased supplier diversification, stimulating both supply and demand, is therefore needed. OpenRAN by its very nature allows technology providers from various states to be incorporated into the supply chain which includes general-purpose hardware, software-defined technology, encompassing RAN, or Radio Access Network, in particular. That is why this technology is also regarded as an opportunity for companies that offer technology solutions from around the world. Currently, OpenRAN rollout is limited to rural and some city and suburban networks; soon it will help set up the so-called private networks too, which are going to be installed in office spaces, shopping malls, stadiums or sports arenas.[38]

OpenRAN started to be endorsed and developed also in the UK and Poland; the cooperation on this technology would better position both countries in its value chain. On 24 April 2020, an inquiry on Security of 5G and Open Radio Access Networks was held in the UK. The inquiry drew attention to the fact that paradigms that underpin the OpenRAN model can contribute to improving the UK's network security both in the existing 3G, 4G or 5G networks and in the upcoming generations. The leading role of British companies in this technical innovation was also described as substantial, not only due to the Telecom Infra Project grouping British carriers Vodafone, BT, Telefónica (O2 UK), but also thanks to OpenRAN component vendors joining the ranks of the Project. In Ipswich, England, the BT-sponsored TIP Community Labs are already running. This physical space allows member companies to cooperate on designing new solutions in the 5G area and beyond. Vodafone has started OpenRAN testing in Great Britain, Ireland, Mozambique and the Democratic Republic of Congo. Telefónica is planning to start testing of OpenRAN for 4G and 5G in the UK, Germany, Spain, and Brazil; it expects OpenRAN commercial deployment to speed up. All this demonstrates that OpenRAN fits into the plans of HM's UK's government, which seeks the country be a global 5G leader. The above-mentioned inquiry, discussed the possibilities for creating a conducive environment for the British OpenRAN market to flourish both in terms of increasing network security and market benefits. To this end, ensuring support, financial and otherwise, for innovative British companies in radio access networks was pointed out as necessary.

On the other hand, the Polish company IS-Wireless is one of the worldwide leaders

35 *Cyberbezpieczeństwo instalacji przemysłowych – fundament projektu „Industry 4.0" i szansa dla Polski*, The Kosciuszko Institute, 2016.
36 *National Cyber Strategy 2022*, p. 35.

37 *NIST Cybersecurity for IOT Program*, [online]: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.
38 Miłkowski A., *Rynek producentów platform telekomunikacyjnych dla sieci komórkowych 5G to szansa rozwoju dla polskich firm programistycznych*, [online]: https://prostoibezposrednio.pl/blog/polscy-programisci- 5g.

in the OpenRAN 5G solutions. As OpenRAN solutions enter the global market, Polish companies see prospects opening up for them to share in the 5G application and service market and telecommunications products. OpenRAN solutions should also be perceived as a chance to develop innovative projects in Poland in cooperation with local governments, municipal companies and firms that base their growth on using cutting-edge technology.

Thus, both countries can consider setting up an R&D fund to boost research and commercial use of OpenRAN solutions including the promotion of secure technology development and inclusion of security functionalities as well as standard-based equipment such as devices developed according to the criteria outlined by the O-RAN Alliance, the Telecom Infra Project, 3GPP or the O-RAN Software Community. The UK and Poland can also enhance cooperation on setting security standards for this new technology and software design as well as industry-wide initiatives that aim to help deploy these solutions on a large scale.

Artificial Intelligence

As mentioned in the National Cyber Strategy (NCS) and Integrated Review of Security, Defence, Development and Foreign Policy, a paramount example of a dual-use technology of key importance to the UK is artificial intelligence, described as 'technology in which a computing system is coded to "think for itself", adapting and operating autonomously.'[39] The UK, through the work of Alan Turing, has pioneered the development of mathematics-driven powers of deduction by machines and has ambitions to remain at the forefront of developing machine-learning algorithms, deep learning, neural networks, natural language processing and other sub-categories of sciences that will be vital to maintaining competitive advantages in the field of emerging technologies. The NCS 2022 mentions several areas in which the use of these solutions will be particularly important, most notably cybersecurity, microprocessor design and securing foreign policy and prosperity interests by leveraging and exporting cyber capabilities.

In a world where data generated by the Internet of Things, social media connectivity and cloud computing, is a valuable asset, its use will be critical to cybersecurity processes. As highlighted in the Government Communications Headquarters' report 'Pioneering a New National Security,' 'an increasing use of AI will be fundamental to GCHQ's mission of keeping the nation safe.'[40] Digitalisation and further automation, embedded into physical objects and infrastructure, will generate a lot more data, which presents challenges for its security. AI algorithms not only need to be safe; they also can improve security in various contexts by outperforming humans in conducting a great deal of computations at once. The NCS 2022 explicitly mentions the use of AI to conduct network monitoring and detect cyberattacks and other malicious activity,[41] working on developing those solutions with Alan Turing Institute.[42] Likewise, AI development will be crucial in responding to AI-generated, ever-changing malware that may soon threat the stability of cyberspace.

These goals are in line with Poland's priorities in developing AI. Poland is already a leader in the Central and Eastern Europe region in human capital and the provision of specialized, higher education courses in the field of AI.[43] Having been named a Digital Challenger by McKinsey, Poland can use digitalisation as its next driver of sustained growth. This is recognised by the Polish government, which works on the implementation of digital solutions by formulating appropriate sectoral policies and setting up the GovTech project to support Polish authorities in finding and defining technological projects.

At the end of 2020, Polish Chancellery of the Prime Minister issueda strategic document 'Policy for the development of artificial intelligence in Poland from 2020' with the aim of creating a holistic AI ecosystem for the benefit of the public and business alike. The ecosystem will be established through the reform of the education system (primary, secondary, and higher level) to provide lifelong learning opportunities in AI-related fields, reinforcing digital infrastructure, regulatory framework and test environments, as well as creating a data ecosystem with trustworthy and high-quality data and increased data exchange mechanisms. The document included over 200 other commitments, including the establishment of permanent cooperation with the United Kingdom in the medium term. Furthermore, in 2019, the Polish AI Tech scientific consortium was established, consisting of top 10 Polish universities intending to educate ICT specialists.

Given the overlapping British and Polish goals in the development of artificial intelligence and the complementary needs of the two countries, cooperation in AI should be implemented at a horizontal level.

Post-Quantum cryptography

Quantum research is another area that could form the basis of the future UK-Poland dual-use technology cooperation. The UK intends to become a world leader in developing these capabilities, due to their incredible transformative potential and the important role they play in securing and advancing the nation's Cyber Power Areas of interest in this field in particular refer to quantum computing, quantum sensing and post-quantum cryptography, as well as further developing National Quantum Technologies Programme., The Programme represents GBP 1 billion of public and private investment,[44] in order to make the UK a centre for research and investment in quantum technologies, to attract and retain talent and drive market growth by converting researchers' scientific work into outputs for public and commercial use.

Quantum technology is extremely important for the future of cybersecurity. It has extremely disruptive potential because quantum computers factorize large natural numbers much faster than classical computers. This poses inherent problems as many commonly used encryption systems rely on the use of one-way mathematical functions. The use of quantum computers for malicious purposes could therefore break many cryptographic applications that are used every day in countless solutions.

At the same time, advances in quantum technology come hand in hand with quantum cryptography, i.e. the use of quantum systems for secure communications. Due to the properties of quantum circuits, any attempt to eavesdrop on quantum communications would be detected after the signal has been received, as a sheer observation of the signal would introduce noise into it. These reasons mean that quantum technologies will be crucial to enhancing cybersecurity and safeguarding state apparatuses and economies. Moreover, due to the possibility of backward-breaking today's ciphers (storing encoded messages in databases for later decryption), the allied powers should focus on implementing quantum encryption as soon as possible, treating it as a matter crucial to their sovereignty.

Poland is a perfect place to develop quantum technologies. Polish scientists have been at the forefront of research into this field for many years, including personal collabora-

39 *Ibidem*, p. 125.

40 *Pioneering a New National Security - The Ethics of Artificial Intelligence, Government Communications Headquarters Paper*, https://www.gchq.gov.uk/files/GCHQAIPaper.pdf, p. 6.

41 *National Cyber Strategy 2022*, p. 80.

42 *Ibidem*, p. 102.

43 *State of Polish AI 2021*, Fundacja Digital Poland, pp. 10–11.

44 *Quantum technologies theme*, [online]: https://www.ukri.org/our-work/browse-our-areas-of-investment-and-support/quantum-technologies-theme/.

tion on major achievements in this field. Poland was among the main initiators of the 10-year European Quantum Technologies Flagship Programme and is a partner of the European Quantum Communication Infrastructure (EuroQCI) Initiative. Poland has already developed research units with significant accomplishments in quantum analysis, including for example the International Centre for Theory of Quantum Technologies (developed alongside scientists from Vienna) and the Centre for Quantum Optical Technologies. The country is also pushing strongly for quantum technologies. On 31 January 2022, an agreement was signed between the International Centre for Theory of Quantum Technologies and Quantum Cybersecurity Hub Europe to create a quantum cybersecurity ecosystem in Poland, while in early February 2022, Poland's Deputy Minister for Digitalisation inaugurated the first quantum hub in Central and Eastern Europe as part of the agreement between IBM Quantum Network and Poznan Supercomputing and Networking Center.

Poland and the UK have a long and illustrious history of cryptologic cooperation. Without the participation of both Polish and British scientists, the Enigma might not have been broken and the fate of the Second World War might have taken a completely different, sinister turn. It is time to join forces again and cooperate on post-quantum cryptographic and cryptologic solutions.

5. BUILDING A ROBUST CYBER SECTOR AND INNOVATION COOPERATION

The cybersecurity sector in the UK is highly innovative, thanks to a large number of innovation centres, industry clusters, and above all, effective public-private cooperation. Polish cybersecurity industry treads the path of dynamic development with a great potential to create innovative solutions utilizing the brainpower of a large number of specialists and STEM graduates. Due to the characteristics of both markets, Polish-British cooperation in fostering cybersecurity innovations has a great potential that needs to be unlocked.

Growing cybersecurity market

The UK's cybersecurity industry is one of the largest and most developed in Europe. With nearly 1,500 cybersecurity companies in operation, it reached a value of nearly GBP 9 billion in 2021. Almost 50,000 people are employed in the sector,[45] and British companies can operate locally, nationally and globally. These figures clearly show the position of the UK cybersecurity industry and its scale. The maturity of this sector is also evidenced by the extensive network of clusters and other industrial organisations supporting the development of this sector. There are about 20 cybersecurity clusters in the UK, which allows for market consolidation and better coordination of pro-export and pro-innovative activities. In addition, there are several centres of innovation support in the field of cybersecurity in the UK (including LORCA, Plexal Cyber, Center for Secure Information Technologies) with extensive ecosystem and support instruments in the form of accelerators and incubators supporting the development of innovative IT-sec solutions in the UK.[46] The UK is highly successful at translating research into innovation and new companies in the areas of technology are most vital to its cyber power. It supports academics across the UK to commercialise and operationalise their research by adopting a more challenge-based approach in collaboration with industry partners. This helps identify ideas with the highest potential and stimulate investment from funders. The scale and maturity of the cybersecurity market in the UK can be a useful benchmark for developing markets, e.g. the one we observe in Poland.

The Polish cybersecurity ecosystem is in the phase of dynamic development. In 2021, its value was estimated at GBP 400 million and it is anticipated that it will grow by approx. 10% annually.[47] Thanks to the dynamic digital transformation in Poland, the supply of cybersecurity products and services will continue to grow, which creates opportunities for building an effective ecosystem within the country. Polish cybersecurity industry is service-based, with more than 50% of companies delivering the related services (mostly audits, consulting and penetration testing). Most of the product providers are non-Polish, which means that importing cybersecurity solutions is still the main strategy on the market, with local integrators and distributors, VARs, playing a pivotal role.

Along with the development of the market, industrial organisations supporting the business and innovation are being created. The Polish Cyber Security Cluster #CyberMadeInPoland was established in 2020, bringing together almost 50 Polish entrepreneurs in the field of IT-Sec.[48] Polish cybersecurity companies are also part of software development organisations.

45 *UK Cyber Security Sectoral Analysis 2021*, Department for Digital, Culture, Media and Sport.
46 *UK Cyber Cluster Collaboration*, [online]: https://ukc3.co.uk/.
47 *Report: Polish cybersecurity market Opportunities and challenges*, Venture INC.
48 *Polish Cybersecurity Cluster* #CyberMadeInPoland, www.cybermadeinpoland.pl.

Polish-British cooperation on cybersecurity innovation

Despite the differences in the size and profile of the market, cooperation in the area of cybersecurity between British and Polish ecosystems is constantly developing. The #CyberMadeInPoland cluster cooperates bilaterally with British clusters on initiatives aimed at making activities international. Joint Polish and British initiatives also have a European dimension, where both ecosystems are involved in the implementation of projects at the European level, supporting the scaling of the activities of cybersecurity SMEs (Secure IT project) or as part of the European Cyber Security Organization activities.

The establishment of the Global EPIC initiative in 2017 was a tangible evidence of cooperation in pursuing an innovative international-cooperation-building approach to cybersecurity innovation and internationalisation. Among the founding members were the key stakeholders from Poland and the UK, including Cyber Wales, the Centre for Secure Information Technologies, and the Kosciuszko Institute. The cooperation within Global EPIC focuses on developing global, paradigm-shifting partnerships and cooperation between members, leveraging cybersecurity to enable economic development and offering companies and entrepreneurs a low risk entry for a trial period in one of the Global EPIC ecosystems. The Global EPIC initiative currently includes 31 cybersecurity ecosystems from around the world, including one from Poland and five from Great Britain.[49] The programme to support internationalisation and entering the British market is also offered to Polish companies as part of the activities the British Embassy in Poland engages in, leveraging the relationships with Polish cybersecurity companies facilitated by the #CyberMadeInPoland cluster.

Furthermore, the internationalisation of Polish companies on the British market is an excellent example of such cooperation and the potential that lies in it. According to the research conducted by #CyberMadeInPoland, almost 25% of Polish IT-Sec companies consider the possibility of expansion into the British market.[50] At the same time, the cybersecurity market in Poland, due to its high business growth potential, is also attractive to British companies. In 2019, 12 British companies visited the CYBERSEC EXPO event in Katowice, where they had the opportunity to meet market participants: companies, end users, industry organisations and public administration. In 2020, almost 40 British companies participated in the remote CYBERSEC EXPO trade fair.[51]

Beyond 2022: joint ventures, soft-landing and EDIHs

As the largest country in the CEE region, Poland has the ambition to be home to the most dynamic and promising cybersecurity innovation hubs. By sharing knowledge and experience, British investors can help to co-create the Polish innovative ecosystem and support the growth of the IT-Sec sector and the scaling up of Polish start-ups. Mutual exchange of experiences or implementation of joint pro-development projects will certainly support and accelerate the Polish-British cooperation in this field. In addition, to better understand the market and to create channels of cooperation, it is worth investing in joint events and trust-building meetings of Polish and British companies or clusters to develop the best possible understanding of the market characteristics.

At the same time, the British market, due to its maturity and size, remains an attractive export destination and expansion destination for Polish companies. In this field, Polish companies can be supported both by the British Embassy, actively involved in the soft-landing process,[52] and some Polish institutions supporting entrepreneurship and exports (Polish Agency for Entrepreneurship Development, Polish Investment and Trade Agency). In the wider European context, it is worth investing in a trade mission and industry events as the most effective instruments supporting internationalisation.

In terms of creating innovation, the role of European Digital Innovation Hubs (EDIH) should also be taken into account. EDIHs are a development of the Digital Innovation Hub concept proposed a few years ago by the European Commission and are intended to support a safe digital transformation of SMEs by offering specialist services in such fields as cybersecurity.[53] While the EDIH program is an initiative of the European Union, collaboration between EDIHs and other digital innovation hubs may go beyond the project itself. The creation of EDIHs specializing in cybersecurity will consolidate a highly dispersed cybersecurity industry in Europe, which in a wider perspective will facilitate contacts and exchange of information between ecosystems. The Polish EDIH CYBERSEC HUB specialising in cybersecurity may become a catalyst for cooperation between innovation centres in Great Britain and Poland. Establishing a relationship in this area will allow for a significant expansion of cooperation channels and the implementation of transnational initiatives for innovation and support in providing cyber solutions in Great Britain and Poland.

Even though the cybersecurity ecosystems of Poland and United Kingdom differ in terms of maturity and size as well as their market characteristics and external conditions, they can still learn a lot from each other. The Polish-British cooperation in cybersecurity has already proved successful, and has a great potential, particularly for creating joint innovations and establishing business relations and investments.

49 *Global EPIC*, www.globalepic.org.

50 Internal research.

51 *European Cybersecurity Forum*, www.cybersecforum.eu.

52 Soft Landing is a dedicated programme helping foreign companies establish business in a chosen ecosystem and accelerate their growth. Usually Soft Landing programmes offer consulting services, industry research, office rental, networking activities, access to finance, etc.

53 *European Digital Innovation Hubs*, https://digital-strategy.ec.europa.eu/en/activities/edihs.

CONCLUSIONS

- Cyberspace has become an increasingly and always contested environment, with malicious actors endangering both international and individual security;
- Polish-British relations, based on historical trust, strengthened political-economic cooperation and cultural blending, may become the basis for expanding cooperation in the field of cybersecurity;
- Cooperation in this area cybersecurity is needed especially now, during the geopolitical turmoil caused by a full-scale invasion of Ukraine by Russia which, alongside countries like Iran and North Korea and more assertive China, poses a significant threat to the international order, national security and the security of cyberspace;
- The bilateral cybersecurity dialogue must be run on a multi-level and multi-sectoral basis, in the diplomatic, ministerial, operational and social fields.
- Since the Treaty on Defence and Security Cooperation between the UK and Poland acknowledges security challenges arising from cyber and hybrid warfare, the cooperation between the two countries should also involve the military aspect and areas such as EDTs or APT prevention.
- Military cooperation should include, inter alia, capability development, information sharing, experience exchange, education, and training.
- The future Polish-British cooperation should focus on developing the technologies needed to expand the cyber power – such as operational technologies, the Internet of Things, OpenRAN, Artificial Intelligence and Post-Quantum cryptography.
- Both countries can also use the characteristics of their digital market sectors to significantly expand the reach and profits of their organisations. The British market is well established, with significant scale and maturity levels. The Polish cybersecurity ecosystem is in the phase of dynamic development. As such, both these markets can complement each other.

AUTHORS' BIOS:

Ciaran Martin

Ciaran Martin is Professor of Practice in the Management of Public Organisations at the University of Oxford. Prior to joining the School, Ciaran was the founding Chief Executive of the National Cyber Security Centre, part of GCHQ. Ciaran led a fundamental shift in the UK's approach to cybersecurity in the second half of the last decade. He successfully advocated for a wholesale change of approach towards a more interventionist posture and this was adopted by the Government in the 2015 National Security Strategy, leading to the creation of the NCSC in 2016 under his leadership. Over the same timeframe, the UK has moved from joint eighth to first in the International Telecommunications Union's Global Cybersecurity Index and the NCSC model has been studied widely and adopted in countries like Canada and Australia. The NCSC's approach has been lauded for responding quickly to incidents and giving the British public clear and prompt advice on responding to them, putting previously classified information in the hands of industry so that companies can defend themselves more effectively, major improvements in automatic cyber security like countering brand spoofing and rapidly taking down malicious sites, and projecting the UK's leadership in cyber security across the world. Ciaran's work, which led to him being appointed CB in the 2020 New Year's Honour's list, has also been recognised and honoured in the United States and elsewhere across the world. In his 23-year career in the UK civil service, Ciaran held senior roles within the Cabinet Office, including Constitution Director (2011-2014), which included negotiating the basis of the Scottish Referendum with the Scottish Government and spearheading the equalising of the Royal Succession laws between males and females in the line; and director of Security and Intelligence at the Cabinet Office (2008-2011). Between 2002 and 2008 he was Principal Private Secretary to the Cabinet Secretary and Head of the Civil Service and Private Secretary to the Permanent Secretary to HM Treasury. As well as secure technology, a constant theme has been the promotion of responsible, values based-Government whether in the Treasury, Cabinet Office or the security services. As a native of Northern Ireland's troubles which he saw in part as being themselves caused by a failure of Government, Ciaran knows the importance of fair, impartial, well run public services that work for all and are trusted. So prior to his NCSC career he is particular proud of his supporting role, along with Ministers and civil servants in London and Edinburgh, in framing the arrangements for the 2014 independence referendum an event which, whilst hotly contested, was seen by all to be fair, legally sound and decisive. His knowledge of public finances, national and international security and the central bureaucracy of Whitehall is a rare combination of experiences and expertise. Ciaran is a Member of the CYBERSEC Programme Committee.

Izabela Albrycht

Izabela Albrycht is a political scientist and graduate of the Faculty of International and Political Studies at the Jagiellonian University in Kraków. She is a co-author of reports, publications and analyses focusing on issues related to EU policies, international relations, cybersecurity and digital technologies. Since 2014, she has been leading the European Cybersecurity Forum – CYBERSEC which she also co-founded. In 2021, she held the position of Chair of the the CYBERSEC Programme Committee. She chaired the Kosciuszko Institute from 2010 to 2021. In July 2020, she was appointed by NATO's Secretary General Jens Stoltenberg a member of the NATO Advisory Group for Emerging and Disruptive Technologies. In December 2021, she became a member of the Advisory Group to the President of the Republic of Poland on security and defence issues. Between 2016 and 2018,

she chaired the Council for Digitization in the Ministry of Digital Affairs and she is now its member in the Chancellery of the Prime Minister. She is a co-founder of Women4Cyber in the European Cyber Security Organisation (ECSO) and the Polish Cybersecurity Cluster #CyberMadeInPoland.

Michał Rekowski

Michał led the Kosciuszko Institute's programme & research activities until June 2022. He was also the Programme Director of the European Cybersecurity Forum – CYBERSEC. Currently, he is preparing a doctoral dissertation on the European Strategic Autonomy at the Department of National Security of the Jagiellonian University in Krakow. Michał is also a Principal Investigator for a research project 'The role of the European Union institutions in building the European Strategic Autonomy' financed by the National Science Center, Poland. Michał's interests are cybersecurity policy and the role of technology in international relations. He focuses on the strategic dimension of the EU's technology policies. He also specializes in the Common Security and Defence Policy of the EU and European security. Michał received a scholarship from the Tokyo Foundation for Young Leaders (2020) as well as numerous other scientific scholarships. He conducted research visits to the King's College London, Vrije Universiteit Brussel, the University of Salzburg, and the University of Heidelberg. Participant of international conferences and author of articles on security and geopolitics, he wrote, among others, for the European Policy Analysis Center, Centre for European Perspective and Forbes. He was an originator, co-author and editor of the experts' report 'Geopolitics of new technologies' (2020). Michał frequents international conferences and often comments on cybersecurity and security events in the Polish media (including TVN24, Polsat, TVP World). In 2018, he did a five-month BlueBook internship at the European Defence Agency. Michał has lived and studied in Brussels (VUB), Paris (SciencesPO), Singapore (National University of Singapore) and Krakow (Jagiellonian University).

Maciej Góra

Maciej Góra is a Project Coordinator of the Kosciuszko Institute. He studied National Security at the Jagiellonian University, Cyber Security at the AGH University of Science and Technology (both in Krakow) and International Relations at the Charles University, Prague. During his tenure at Kosciuszko Institute he coordinated multiple initiatives and projects, creating and operationalizing multiple points of agenda of European Cybersecurity Forum – CYBERSEC, leading the engagement of KI during Internet Governance Forum 2021 and IGF Poland 2022, co-authoring the anti-disinformation textbook for high schoolers and textbook for teachers, participating as guest and as a host in General Talks podcast and more. His research and professional interests include digital and cyber issues on a micro (reducing digital footprint, personal online safety) and macro scale (geopolitical dimension of cyber security, cyber security management, social pro-cesses related to digitalization, futurology).

Łukasz Gawron

Łukasz Gawron is a graduate of International Relations at the Jagiellonian University in Krakow, where he also completed his BA studies. He coordinated the European Energy Hub project at the Institute of Public Policies. For many years associated with the Kosciuszko Institute, where he was responsible for organizing several CYBERSEC events and projects coordination. Since 2021, he has been a deputy chairman, and currently Chairman of the Polish Cybersecurity Cluster #CyberMadeinPoland. In the cluster, he is responsible for business development, project supervision, relations with partners and management. He has a PRINCE2 Foundation project management certificate.