The Polish Quarterly of International Affairs

volume 24 no. 3/2015

International Criminal Court —the Central Figure of Transitional Justice?
Tomasz Lachowski

TTIP's Monetary Clause Muddle
Maria Dunin-Wąsowicz, Katarzyna Żukrowska

APT—the New Cyberforce?
Matteo Casenove, Kaja Kowalczewska

Serbia's Challenges on the Way to the EU
Bartosz Marcinkowski

PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

The Polish Quarterly of International Affairs

volume 24 no. 3/2015

PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

Managing editor: Kacper Rękawek
Copy editor: Anthony Casey
Proof-reading: Katarzyna Staniewska
Cover design: Malwina Kühn
Typeset: Dorota Dołęgowska

Contributors:

Matteo Casenove—malware analyst, independent researcher, Italy

Justin Dunnicliff—analyst, U.S. Department of Defense

Maria Dunin-Wąsowicz—Ph.D., board member, European Movement Forum

Paulina Iżewicz—research analyst, International Institute for Strategic Studies (IISS)

Kaja Kowalczewska—lawyer, Ph.D. candidate, Jagiellonian University in Kraków

Karolina Kuśmirek—Ph.D. candidate, Maria Curie-Skłodowska University (UMCS)

Tomasz Lachowski—Ph.D. candidate, University of Łódź

Bartosz Marcinkowski—assistant editor, *New Eastern Europe*

Paweł Tokarski—Ph.D., senior associate, German Institute for International and Security Affairs (SWP)

Lee Turpin—Ph.D. student, Lancaster University

Anna Visvizi—Ph.D., assistant professor, DEREE-The American College of Greece; research fellow, Institute of East-Central Europe (IESW)

Dawid Walentek—economics graduate, University of Amsterdam

Katarzyna Żukrowska—professor of economics and political sciences, Warsaw School of Economics

Publisher:
Polski Instytut Spraw Międzynarodowych (The Polish Institute of International Affairs)
ul. Warecka 1a, 00-950 Warszawa;
tel. +48 22 556 80 00; fax +48 22 556 80 99; e-mail: pqia@pism.pl

ISSN 1230-4999

The Polish Quarterly of International Affairs is regularly presented in the catalogue of International Current Awareness Services, in Ulrich's International Periodical Directory, and in International Political Science Abstracts/Documentation Politique Internationale. Selected articles are included in the International Bibliography of the Social Sciences.

Edition: 350 copies. Sent to press in December 2015
Printed by Ryko, ul. Piłsudskiego 17, 05-480 Karczew

CONTENTS

ARTICLES

Matteo Casenove, Kaja Kowalczewska
APT—the New Cyberforce? 7

The authors explain the Advanced Persistent Threats (APT) phenomenon in the context of the legal and technical one perspectives. The APT definition is juxtaposed with the legal term of armed attack. Legal reflections are concentrated on the characteristics of the APT and try to explain whether this category is sufficiently unambiguous and consistent to serve as a powerful argument in legal analysis, which is especially important to the decision-makers in the context of self defence and the legality of a military response to a cyberattack. The technical perspective adds complexity to APT analysis due to the intrinsic characteristics of the malware, and more generally of the cyberattack. Therefore, the authors argue, analysis cannot merely focus on the technical context, and they underline the necessity for integration with the geopolitical and military context in order to provide a more exhaustive view of the attack and to support the attribution process.

Justin Dunnicliff, Paulina Iżewicz
Civilian or Military? Addressing Dual-use Items as a Challenge to the Nuclear Non-proliferation Regime 21

Various efforts have been made to establish export controls and other mechanisms that would prevent illicit nuclear trade from occurring. These tools have been fairly successful in capturing illicit transactions of goods whose application is purely nuclear. The goods and technologies that can be used for both military and civilian purposes, the dual-use items, remain the key challenge. The legitimate market for such goods is enormous, but they also have applications in centrifuge, laser enrichment, reactor, and plutonium separation programmes. Iran and other proliferators have a long history of attempted procurements in this area, including items such as valves, frequency converters, carbon fibre, machine tools, and many others. The current non-proliferation regime has been slow to catch up with this reality. It is crucial to reverse this trend and adapt international standards, to provide a more holistic approach to countering nuclear proliferation.

Karolina Kuśmirek
Polish Special Operations Forces:
Role and Missions in Afghanistan 31

Polish Special Operations Forces have participated in missions abroad, for example, in Afghanistan. In the initial phase, special forces soldiers were assigned to the tasks that could be performed by conventional military units, such as protection of bases, but over time the situation changed. Their actions contributed to stabilising the situation in the region and indirectly resulted in increased international security. During the operations, soldiers released hostages and confiscated weapons. In this way they disrupted the opponent, because the losses incurred by terrorists led to the depreciation of the position of the leaders of the terrorist networks. In addition to special operations, soldiers were preparing "Afghani Tigers" officers to carry out activities independently, and to ensure safety after the coalition forces left the region. Cooperation of soldiers with the Afghan officers is the proof of success in building positive relationships. Implementation of special operations by special forces soldiers led to their gaining new experience, and to the modernisation of armaments and verification of procedures. The activities conducted proved that Polish special forces are a reliable partner.

Tomasz Lachowski
International Criminal Court—the Central Figure
of Transitional Justice? Tailoring Post-violence Strategies,
with Special Reference to Ukraine 39

This paper is devoted to analysing the factual and potential influence of the International Criminal Court (ICC) in a conflict and post-conflict environment. It is argued that the ICC's capacity has to be measured by its ability to tackle the "hard-cases," both geopolitically and legally, and to serve as a real means of implementing transitional justice strategies applied by post-violence societies. The initial evaluation of the ICC's capacity in the field of international and transitional justice is compared with the current situation in Ukraine, since Kyiv has lodged two ad hoc declarations under Article 12 (3) of the Rome Statute. The first accepted the jurisdiction of the ICC with reference to "Maidan crimes" that occurred during the winter of 2013 to 2014, and the second covers the possibility of crimes against humanity and war crimes committed in the course of warfare in the Donbas region. Undoubtedly, careful analysis of the ICC's presence in the Ukrainian crisis is required.

Bartosz Marcinkowski
Balkan's Bad Boy Goes West:
Serbia's Challenges on the Way to the EU 59

Since the Balkan Wars in the 1990s, Serbia has been perceived by Europe as its enfant terrible. This is an effect of Serbian war crimes, of an unwillingness to cooperate with the International Criminal Tribunal for the former Yugoslavia, and general reluctance towards Western political structures in Serbian society. The tension between the West and Serbia grew particularly high in 1999 during the NATO bombing of Yugoslavia, and in 2008 when Kosovo proclaimed independence. In spite of these tensions, within last few

years Serbia has been successfully involved in a normalisation process with Kosovo as a part of its rapprochement with the EU. Serbia has opened itself to the West but it still maintains good relations with Russia, regardless of the Kremlin's foreign policy activities. Hence, the author argues that rethinking relations and cutting certain ties with Russia should be among the key conditions for Serbia to join the EU, no less important than normalisation with Kosovo.

Paweł Tokarski, Anna Visvizi
Poland's Winding Road to the Eurozone:
From a Cost-Benefit Stance to Risk Aversion 65

More than a decade after EU accession, Poland, an initial enthusiast of euro adoption, has turned into merely an assertive endorser thereof, with the prospect of Polish entry to the eurozone vanishing over an uncertain political horizon for the foreseeable future. Although legally bound to adopt the euro, Poland has drawn on the indeterminacies built in to the Maastricht convergence criteria to effectively postpone eurozone entry. While the euro adoption initially constituted a predominantly legal challenge, today it is an essentially a political issue. Moreover, as a result of the eurozone crisis, the debate on euro adoption switched from a sober cost-benefit analysis to a political risk (and cost) assessment, where the attainment of nominal and legal convergence has become a function of the Polish government's broader domestic and European political strategy. The outcome of the presidential election in May 2015, described by commentators in terms of an epochal change, further blurs the prospect of Poland's euro area membership.

Lee Turpin
The Europeanisation of British Security Policy 85

This paper considers the impact of British membership of the European Union (EU) on the development of an EU security policy through the Common Security and Defence Policy (CSDP), and on the security policy-making of the British state. It does this through utilising a framework of Europeanisation, whereby policy is both uploaded from the national level to the EU level, and reciprocally downloaded from the EU level to the national level. I argue that this has played a role in shaping British approaches to security policy, whilst ensuring that the CSDP has been clearly positioned to support, rather than supplant, NATO as the premier security organisation in Europe.

Dawid Walentek
South African Politics after the Mangaung Conference 91

The author delivers a perspective on the economic and foreign policy outlook for South Africa with respect to two events that determined the course of South African politics: the ANC conference in Mangaung and the 2014 general election. The motivation for this research is the importance of the ANC in relation to South African domestic politics and the foreign and economic policy, bearing in mind that the ANC has won all elections in South Africa since the end of Apartheid. The study is qualitative and the analysis is rooted in political realism, with the self-interest of individuals as the definitive factor. The author focused on factional tensions within the ANC and changes

in South African political landscape. The key finding is that domestic politics in South Africa are more fragmented and polarised after the Mangaung conference. This is a result of the ANC abandoning nationalistic rhetoric. Nevertheless, the ANC's supremacy in South African politics is unequivocal. South African economic policy will be directed towards business and foreign investors. Foreign policy will drift away from the "African solutions for African affairs" paradigm, and towards limited involvement. In the current global economic, climate South Africa will experience slow economic growth.

Maria Dunin-Wąsowicz, Katarzyna Żukrowska
TTIP's Monetary Clause Muddle 107

We argue that TTIP negotiations, which are focused on improving conditions for mutual trade and investments between the U.S. and the EU, have overlooked the issue of the influence of monetary and exchange rate policies of both sides on the potential results of a prospective agreement. Thus we demonstrate that the agreement should have been supplemented by a monetary clause (MC) in order to avoid a possible mismatch between U.S. and EU currencies. Such a clause, and no other possible currency related legal instruments, should be broad, and aim to regulate the bond between the dollar and the euro. It can work as a convenient springboard to invigorate the multilateral trade system via the institutional nexus of the IMF, WTO, OECD or G-20. The clause can make the agreement as important for strategic relations between the U.S. and the EU as the Treaty of Rome was for the rise of European integration.

REVIEWS

Fredrik Erixon, Krishnan Srinivasan (eds): Europe in Emerging Asia: Opportunities and Obstacles in Political and Economic Encounters (**Krzysztof Iwanek**) 119

Patrick Cockburn: The Rise of Islamic State: ISIS and the New Sunni Revolution; Charles Lister: The Islamic State: A Brief Introduction; Jessica Stern, J.M. Berger: ISIS: The State of Terror (**Kacper Rękawek**) 122

MATTEO CASENOVE, KAJA KOWALCZEWSKA

APT—the New Cyberforce?

Modern Types of Cyberthreats

Today, it is impossible to imagine a military, political or economic strategy without technology to simplify and streamline everyday operations and process massive amounts of more or less confidential data. Even though the idea of a new kind of battlefield, devoid of conventional arms, tanks and aircraft is at best a distant reality, the emergence of the cybercommunity and its governance is inescapable. Technological evolution is instrumental in the improvement of efficiency in all spheres of public governance, but, at the same time, information and infrastructure are being exposed to permanent risks, and are potential target of any player with sufficient skills or resources. In recent years, the scale of such threats has been demonstrated by Stuxnet, Flame, Red October and other malware representing a fracture in cyberattack tactics.[1] These kinds of malicious software are the weapons in national cyberespionage campaigns and critical infrastructure attacks, slowly and silently building up to the next generation of cyber conflicts.[2] These high profile and high-risk campaigns are usually identified and classified as Advanced Persistent Threats (APT).

An APT is a sophisticated, targeted attack against a computing system containing a high-value asset or controlling a physical system. APTs often require formidable resources, expertise and operational orchestration.[3] States

[1] N. Virvilis, D. Gritzalis, *The Big Four—What We Did Wrong in Advanced Persistent Threat Detection?*, Eighth ARES Conference in Regensburg, 2013, pp. 248–254.

[2] C. Tankard, "Advanced Persistent Threats and How to Monitor and Deter Them," *Network Security*, vol. 2011, pp. 16–19.

[3] A. Juels, T. Yen, *Sherlock Holmes and the case of the advanced persistent threat*, Fifth LEET USENIX, 2012, p. 2.

are the most aggressive prospective perpetrators since they have all the capabilities to design and execute such attacks.

The acronym APT is composed of three words describing the main characteristics of the malware or campaign. "Advanced" refers to the complexity of technologies used by the malware, such as tailored social engineering techniques. "Persistent" refers to their stealth and ability to remain undetected for a long period, and "Threat" represents both the capability and intent of a given operation. But is the definition of APTs and the malware that falls under this umbrella unambiguous and consistent enough to serve as a robust argument in the legal analysis?

APT's Already Revealed

Numerous types of malware have been classified as APTs, and each of them possess all or almost all of the characteristics previously presented. Stuxnet, intended to attack the Natanz uranium enrichment plant in order to slow down and sabotage the Iranian nuclear programme, was the first most dangerous and complex threat detected and analysed.[4] This completely autonomous "fire and forget" weapon succeeded in causing physical damage to the Iranian critical infrastructure. The author of this highly sophisticated malware (an alleged joint venture between the U.S. and Israel) had the requisite connections and resources to access restricted and undisclosed information. Although the attack did not cause injury or harm to any human, it had the potential to do so.

Another example is Red October, representing probably the most advanced and intricate cyberespionage campaign seen thus far.[5] The malware was aimed at gathering data from devices and computer systems, infecting diplomatic, governmental, and scientific organisations from all over the world. Extremely complex architecture was used to extract and collect the information, and for five years it evaded detection and extracted hundreds of terabytes of data. Currently, there is no evidence linking the Red October campaign with a particular state. However, the stolen information was top-level data (the malware referred to file extensions used by several

[4] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, 2011, pp. 49–51.

[5] M. Braganca, "Hunt for Red October: The New Face of Cyber Espionage," *SIAK-Journal*, 2013; "The 'Red October' Campaign—An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies," *Kaspersky Lab Expert*, 2013.

international organisations, such as the EU and NATO), and was obviously of great interest to any national intelligence agency.

The Kimsuky Operation is another espionage campaign classified as an APT. Interestingly, this campaign uses very simple and basic malware. According to the analysis,[6] the malware targeted organisations linked to "The supporters of the Unification," an organisation in South Korea and China. This indicates a political context and establishes a framework for a discussion on the relevance of APTs in modern geopolitics.

Late this year, the MiniDuke[7] campaign was detected again, operating after two years of inactivity, under the new name of CosmicDuke.[8] This new version appears to have a very wide range of espionage interests. It targets information from organisations involved with government, diplomacy, energy, telecommunications, and military sectors, operating in states such as Georgia, Russia, the United Kingdom, Kazakhstan, India, Belarus, Ukraine, Cyprus, and Lithuania. The complexity of the malware and the countries in which the infections have been detected lead researchers to assume that it is a state-sponsored campaign. In particular, documents explicitly referring to political issues, such as the recent crisis in Ukraine and NATO operations, have been found during the investigation. These findings, along with little language clues left in the code suggest that CosmicDuke is part of an international cyberespionage campaign carried out by Russia. However, this cannot be proved with absolute certainty.

An APT is much more than a complex piece of code; it is potentially damaging piece. It does not matter whether it is a professional or elementary, as long as it is effective and critical. The "Advanced" attribute given to an APT is represented by the selectivity of its targets, which also expresses its imminence. The classification of an APT is far more complicated than simple malware analysis, since it requires much more sophisticated study, which does not end with simple code analysis. To understand the critical nature of a target or the possible motivations behind an attack, human involvement together with technical, political, and military skills are required. Unfortunately, the analysis itself is not an exact science, and due to the physical diversities of

---

6 D. Tarakanov, "The 'Kimsuky' Operation: A North Korean APT?," *Kaspersky Lab Expert*, 2013.

7 C. Raiu *et al.*, "The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor," *Kaspersky Lab*, February 2013.

8 "COSMICDUKE: Cosmu with a twist of MiniDuke," *F-Secure Lab Security Response*, July 2014, www.f-secure.com.

the APT samples, it is impossible to create a common analysis framework for the classification of APTs. What unifies them is their political nature, which in consequence raises a legitimate question as to the possible response of an attacked state, and proves that only a limited category of cyberevents may subject to legal analysis.

Bytes, Bullets, or Both?

Under the regime of the UN Charter, the use of force is considerably limited, although not totally excluded. The phrasing of the UN Charter, combined with five different original language versions, does not make the analysis of APTs any easier. A careful reader will soon conclude that the Charter refers to various notions without explaining them, and, what is more, displays to some extent a lack of internal cohesion when it comes to the concepts such as "use of force," "use of armed force" and "armed attack." In the mid 1940s, the international community at least agreed that the notion of the use of force did not include the use of economic dominance, as postulated by countries from the Soviet bloc, and would be limited to the conventional use of armed force.

Consequently, Article 51[9] and Chapter VII[10] are the only basis for defining a legally accepted threat or use of force, though they do not provide the international community with a precise definition of either. According to the general approach, the category of "armed attack" constitutes a qualified sub-category of the wider term "use of force." One of the approaches is also the negative definition of armed attack, as an act crossing the threshold of Article 41 of the UN Charter. This states that the following actions cannot be classified as the use of armed force: "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication [which, nowadays, we would understand to include mobile phone networks and the internet as well], and the severance of diplomatic relations." Consequently, an armed attack is qualified as a somehow more serious act, which reaches a relevant threshold of seriousness.

[9] "Nothing in the present Charter shall impair the inherent right of individual or collective self defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security....," Art. 51, UN Charter.

[10] Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression.

The other approach results from the judicial activity of International Court of Justice (ICJ), which is faced with the challenge of defining an all-embracing notion of armed attack that can be applied to different cases,[11] but which has so far failed to satisfy the international community's need for a decisive resolution on the exact designation of an armed attack. However, it should be noted that one of the incentives underlying the ICJ's narrow approach towards armed attack is to limit a state's unilateral decision to use of self-defence, which could easily lead to an escalation of a crisis into an armed conflict.

Consequently, an armed attack as well as a mere response to it, in self defence, has to be examined separately in each case, for example, by referring to the guidelines drawn up by the ICJ. Especially if such an attack originates in cyberspace,[12] a new type of battlefield, such an interpretation may be more than challenging.[13]

The notion of a cyberattack has recently gained a lot of attention, particularly from the military and public authorities concerned with the security of critical infrastructure. This was demonstrated by the adoption of a new cyberdefence policy and accompanying action plan by NATO defence ministers in June 2011,[14] and the current project of NATO's Cooperative Cyberdefence Centre of Excellence in Tallinn, which aims to revise the 2013 Tallinn Manual.[15] Also, the EU adopted the Cybersecurity Strategy for the European Union,[16] and the European Commission submitted a proposal for a Directive on Network and Information Security,[17] in order to "put forward

[11] ICJ, Nicaragua v. United States of America, Merits, 1986, para. 176, the Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, 1996, paras 41–48, Islamic Republic of Iran v. United States of America, 2003, para. 76, the Palestinian Wall Case, Advisory Opinion, 2004, para. 139, Democratic Republic of the Congo v. Uganda, 2005, para. 145.

[12] One of the classical definitions is framing cyberspace as "computer networks + people + procedures."

[13] U.S. Department of Defense, *Quadrennial Defense Review Report*, February 2010, pp. 37–45.

[14] *Defending the Networks: The NATO Policy on Cyber Defence*, 2011, www.nato.int.

[15] M. Schmitt (ed.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013.

[16] European Commission, *Communication on a Cybersecurity Strategy of the European Union—An Open, Safe and Secure Cyberspace*, 2013, http://ec.europa.eu.

[17] European Commission, *Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union*, 7 February 2013, http://ec.europa.eu.