

NEW CHALLENGES FOR A FUTURE STATE DEFENCE

Fabian BAXA, Ph.D.,

Colonel (Ret), Academic Fellow, University of Defence, Brno, Czech Republic.
E-mail: fabian.baxa@unob.cz

Mgr. Aleš TESARŮ,

PhD Candidate, Lt. Colonel, Research Fellow, University of Defence, Brno, Czech Republic.
E-mail: ales.tesar@unob.cz

Abstract: *There is an increasing number of non-state actors acting recently as well as present armed conflicts aside of state actors when non-state actors being endowed with more economic and “military” power than smaller states what enable them a broad spectrum of activities in all domains explored by human civilisation. Nowadays even an inner space belongs already to activities of non-state actors. Cyber space is an arena of these actors since the beginning of its exploitation. Putting together, it is necessary to expect a growing number of frictions among various state and non-state actors having their own interests in the same areas and time. These frictions may lead to conflicts, even armed conflicts being presented by other activities than engagement of traditional armed forces against property or interests of both, state or non-state actors with an aim to gain some advantage. Actions in an inner space or in a cyber space could be more serious than small scale armed conflict. These actions might be considered as simple criminal or terroristic acts or as casus belli, like consequences of the 11th September 2001 situation. Who is in charge of judging a nature of the offensive actions between two non-state actors? What state is authorised to declare “war against terrorism” (or criminality?) towards one or all belling parties, which are non-state actors? This situation can arise more questions and this article has an ambition to elaborate some of them to address new challenges in the field of future state defence.*

Keywords: *advanced technologies, armed conflict, commercial companies, international law, private security companies.*

Introduction

Global security arena is continuously developing environment and this permanent changes have their reflections in an international legal arrangement. Among the others, one of important dimensions of these changes are actors playing their roles in accordance with their missions, ways and means, which can differ from roles of other, more traditional actors, internationally recognised states.

This article has an ambition to present results of research focused on two groups of relatively new actors of international scene, which already play important roles and these roles are going to be even more important in close future. The international legal environment should adapt itself in order to formulate clear rules how to treat these new actors to keep rule of law in these changeable environment.

The first group of relative actors are *private military and private security companies* (PMCs and PSCs) that are more and more officially used within running armed conflicts trying

to influence a concrete conflict or even to act officially on behalf of an internationally recognised government. The second group of new actors are international or national *private, commercial companies*, which capabilities exceed those within majority of ordinary states. This fact is important from the security as well from military point of view. Therefore, it is only the matter of time when these capabilities would be used in future armed conflicts on behalf of a concrete state or directly in order to enforce interests of the concrete company.

Concerning the first group of actors, they have been already active in recent as well as present running operations and with a high probability it is necessary to calculate their participation in future operations worldwide. There is not only in growing spectrum of these actors but their range of capabilities is also enlarging. These actors are not active in the area of operations in general, their activities can be monitored even during an ordinary, day-by-day life.

The second group of actors, international or national private, commercial companies, have capabilities in a scientific research, industrial production, international trade and turnover higher than smaller states. The reality is that resources devoted by private sector to the science are higher than by states in general. Some of these companies have dominant position in global trade in specific areas, e.g. software, including operational systems for personal computers used almost everywhere. Other companies from this group are even capable to launch missiles with human crew to the space, the capability owned by couple of states only. Both groups of actors are also considered as potential actors of hybrid threats.

Actors from both groups already have an intent as well as capabilities to act in the international arena as states and this trend is more and more clear. It brings new situation to the international legal environment and new challenges for ordinary states and international organisations acting in security and defence areas.

This article analyses the actors in the present and expected security environment and indicates proposals how to deal with expecting problems mentioned in analytical part. The intention is to address this issue and, by mentioning and analysing several typical examples from the recent and present period, to indicate a possible solution, both national and international level. The goal of this article is not to present universal solution of described situation and briefly analysed circumstances but to name the problem. Therefore, there are more questions than answers.

1. Private military companies within the present security environment and related trends

As mentioned in previous parts the main effort is paid to two groups of relatively new actors at the international security arena. This chapter offers several typical examples from both groups with short findings.

The first group contents private, commercially based companies focused on military or security capabilities offered to other actors of international security scene like states or international/national companies to solve assigned tasks. The existence of this kind of companies is not new, throughout history there are many examples of using existing or ad hoc organised groups that hiring former soldiers for hidden missions without discovering customers. In recent European history there are more pieces of information regarding presence of “*furtuna soldiers*” at all sides of an armed conflict in Balkans – Serbian side, Croatian side as well as Bosnian/Muslim side.

Nowadays, the new thing is that there are groups acting openly, even officially on behalf of their customers, like private battalions fighting in South-Eastern Ukraine (UKR) (Holcomb 2016, 33-71) since 2014. It is possible to say that due to lack of regular forces prepared in an appropriate state of readiness a Ukrainian government required several battalions organised, equipped, trained, paid, and owned by national physical persons. UKR General Staff tried to

keep control over these units with some problems associated with misuse of power against inhabitants of troubled areas, using of inappropriate power like extensive rocket launchers fire against inhabited areas, etc. The UKR government proclaims these inhabited areas as inseparable parts of the UKR territory. The main problem of engaging these battalions became when some of these units openly disobeyed orders of the UKR General Staff and marched with their small weapons in protest against the decision of the Kiev government in order to enforce their requirements. Lessons learnt from this situation are that private units can change their opinion quite quickly what may cause a serious problem.

Another example of an engagement of PMC is presence of a Wagner group in Syria (Bahgat 2021) as well as in Mali (Schwikowski et al. 2021). This group has been invited by a local government to fight with rebels in the country. Actions of this PMC included also offensive actions and there are connected with misuse of the power of the group towards local civilians and even mutiny to death of captured persons. Officially, this PMC is not connected to any country, but the owner of this group is from an inner circle of the President Putin therefore it is not far to the verity the group may act as an unofficial tool of foreign policy of the Russian Federation (RF) (Katz et al. 2020). Similar arguments are possible to find also here (GlobalSecurity 2021). The aim of this effort might be to keep Russian influence in several parts of the world supporting the idea of RF as a real superpower. Another unofficial goal might also be to keep a capable combat unit for potential use in future.

The third illustration of the recent activities is an example of the size of PMCs is American presence in Afghanistan where more than one half of a total personnel (Miller 2010) were contractors hired by the US authorities to work in support of the American presence there. These contractors conducted a broad spectrum of supportive tasks, from protection of US and NATO military facilities and bodyguards of VIPs to jobs in logistics, communication and information systems (CIS). There is not information concerning the use of these employees for offensive actions. It seems that the USA has learned a lesson from the engagement of PMCs in Iraq where, due to lack of training, members of the Blackwater company opened fire during a traffic jam at one of the junctions in Iraq.

In accordance with general observation the humanitarian law or the law of an armed conflict there are only two groups of personnel officially acting in armed conflict, military personnel and freedom fighters. A status of employees of PMCs is not specified because they do not belong to these groups. In addition, they are not counted as supportive civilian personnel because they are hired to use weapons for fighting. Using a general explanation of the military personnel when adjective “military” is connected just to the state, private companies have not a status of the state, therefore they cannot recruit and hire military personnel, just civilian employees.

Concerning the use of weapons for civilian personnel there is a generally valid rule that they may use weapons for self-defence or for defence of an object entrusted to care. Within an ordinary state just military units and Police may use weapons for offensive actions and employees of PMCs are not any of them. Therefore, it is hardly possible to find a right legal argument for the use of PMCs as a military unit without blessing from a government. The use of offensive actions on behalf of a private company or under tasking of leaders of a private company might be considered as an illegal use of power.

At the end, the presence of employees with weapons during armed conflict is problematic directly for these employees when captured hence they are not military soldiers or freedom fighters and without strong support from the hiring state, they could be treated as armed criminals.

There is a several partial findings regarding PMCs and their use in recent and running operations. The first is that there is no guarantee to ensure covered or opened disobedience of

such company especially when this company consists of volunteers from several nations. The second is that PMCs can be used in both defensive and offensive actions, which might be problematic according to present rules. The status of their personnel within armed conflict is not clear enough and various countries may see it differently.

In a case of the PMC hired by a government of a foreign state to suppress rebels, that misused its power and tortured captured citizens of this state and other states on hiring state territory, two questions may occur:

- What is a share of responsibility of the hiring state regarding this misuse of power from the side of the hired PMC?
- Who is responsible for protection of civilians when the state administration is not strong enough or not willing to do that?

Naturally, the state should be responsible to protect its citizens anywhere in the world, but if the state measures are not sufficient that state should be considered as a failed state and appropriate international organisations might take over the role of that failed state.

PMCs are considered as one of groups of actors mentioned in hybrid threats and hybrid warfare (HT/HW) papers as a tool for overt and covert subversion actions against the targeted state. Weissmann with his seven dimensions of the hybrid threats and hybrid warfare (Weissmann 2021, 65-67) is one of authors, which are worth being stated.

The PMCs are considered as an instrument of the hybrid threat stated already in the previous US Army Hybrid Threat Force Structure Organization Guide (Headquarters Department of the Army 2015, 2-9-2-17), issued in 2015.

Activities of these organisations are organised at the edge of an open armed conflict and hidden grey zone as actions under threshold of a regular war.

In conclusion of this analytical part, it is possible to formulate following finding:

Although PMCs are entirely new group of actors, their behaviour has been considerably changed. Today they act more overtly even they act directly in armed conflicts, often on behalf of concrete governments as a part of regular, state-controlled armed forces. Their members might face situations like soldiers of regular armed forces, e.g. captivity, but their status is not fully recognised by the present legislative framework. On the other hand, their members very often have problems with loyalty and obedience as well as with compliance of rules of armed conflict.

2. Civilian commercial companies, the present security environment and related trends

The second group of new actors consists of international or national commercial companies with capabilities exceeding those of majority of states in general, and in concreto, their “military-like” capabilities may be larger and more powerful than those of small or medium-sized countries. The first example are private companies with a capability to produce, launch and operate space equipment for their purpose (Rauenzahn et al. 2020). Recently one of these companies presented successfully its ability to launch missiles with a human crew to the inner space.

States and other private companies may hire this capability to satisfy their needs and interests and, on the contrary, other states and private companies may see it as a threat to their interests. Within the space where present traffic is already of quite high intensity then might occur an incident where the private satellite may crash into other, state-owned apparatus, which that state may consider as vital for its interests. There is a first question coming from this situation:

- When the private commercial organisation registered on the territory of one nation would launched attack with a use of weapons on a state-owned object on the territory of other state would it be considered as an armed attack against the state?

NATO Allied Command for Transformation (ACT) released several editions of a paper named Strategic Foresight Analysis (SFA) (NATO Allied Command Transformation 2017, 27-

28), where a situation of state - non-state actors conflict as one of possible crisis in future is mentioned. Even today, it is possible to find some examples of frictions between states and their organisations with commercial companies and once these frictions could convert into a direct conflict or even into the conflict with use of armed violence, concretely weapons. Especially in a situation of a cyber-attack where a definition of a weapon and an armed violence becomes much broader than before.

There are commercial companies devoting more financial resources for scientific research than majority of states therefore in future is possible to expect that these companies will be leaders of a progress in technology. Due to this fact, these companies might have bigger desire to control larger portion of global resources than many of states. Hence, a literature of political science considers willing and means as two necessities to launch hostility.

A similar example could be seen in a position of producers of critical elements of all modern electronics, like microprocessors and memories as well as electronic parts for any larger systems or constructions using any CIS parts, with the Industry 4.0 is critically depended. It is possible to join problems with Covid-19 pandemics negatively influencing not only production but also worldwide transport on a daily basis.

In addition, more than 70% of personal computers (PCs) in the world runs on one common operational system and majority of these PCs use a common office software and are connected to internet using routers and other network parts produced by several commercial companies. In some authoritative regimes, these producers might be influenced to satisfy interests of their administrations. It means there is a growing potential to be not only monitored but also to be targeted directly or indirectly as objects of blackmailing or objects of a cyber-attacks. Simply said, when a concrete commercial company having feeling that its interest are not filled up sufficiently they might misuse its world monopoly to organise hidden or open attack against interests of users regardless they are state organisations, commercial companies or private users. These attacking organisations may also work under command of their government. These attacks might be originally thought as attacks under threshold of armed attacks but targeted states might regard them as *casus belli*. This approach was already declared in a communique from NATO Summit in Wales in 2014 (NATO 2014).

The situation described above induces next question:

- Are states responsible for activities of commercial subjects registered and based on their territory?

At common conditions, regulations for all commercial subjects' operation of the state territory are parts of concession given to these subjects and state authorities are empowered to monitor activities of these subjects and, when necessary, may enforce fulfilment of set up rules. Similarly, when the state allows activities of international commercial subjects registered abroad on its territory it would have to setup an appropriate legal framework. Breach of this framework will lead to a trial where the whole company and/or their managers might be prosecuted. Problem may occur when the commercial subject is registered in some tax-paradise country where the local government is not keen to lose any income and therefore this registered subject breaching rules in other countries is not brought to responsibility. The reason might be simple – the local government is not strong or willing enough to enforce any rules towards registered companies. This situation leads to the next question:

- Is the state of registration responsible for abroad activities of registered companies and what are ways to bring this state to responsibility?

A similar situation appeared in Afghanistan (AFG) with a terrorist organisation named Al Qaeda, which members committed attacks on the USA territory. The USA asked AFG government to release perpetrators to the justice and to close down Al Qaeda facilities on AFG territory. When AFG government refused the USA within their “war against terrorism” recognised this refusal as *casus belli*.

The contemporary international law recognises that a status of war is possible to declare only by a state to another state or states not to a private organisation and it is not important whether terrorist or criminal one in its nature.

Taking into account a fact that a commercial company has not the same status as states in the international scene, therefore a commercial organisation is not possible to be in hostility neither with the state nor with other private organisations. The reason is simple: just the state has a territory, the private organisation may be an owner of a concrete part of the territory of the state. This organisation can sell its territory to another commercial company, physical person or to the state but not to another state. All parts of territory owned by any private organisations belong to the concrete states.

Responsibility of the states for activities of commercial companies using their facilities on the territory of the concrete state has been already mentioned and this situation leads to the next two questions:

- What might these states expect when these companies negatively influence interests of other states?

- Will it be a sufficient and internationally acceptable *casus belli* justifying an armed attack on a facility of the company located on the territory of the other concrete state?

Nowadays, this kind of the attack would be considered as an armed attack against a state territory and it may lead to an armed conflict.

There is also a possibility of damaging activities of international commercial companies outside of the territory of their homeland, the territory where these companies have their general management and headquarters (HQ). These actors may have their facilities on territories of other states, even on the territory where their targets, objects of their negative influence, are located. Typical example is a network of computers-zombies remote controlled from the company located on the territory of completely different state. This network might be used against a vital object of the targeted state causing damages higher than a small-scale armed conflict. Besides the clear responsibility of originator of the attack in this case is questionable what is sharing of responsibility for consequences of the attack among owners and users of remote-controlled PCs and management of attacked objects. The owners of remote-controlled computers did not pay enough attention to protect their computers and managers of attacked objects did not devote enough effort to have their protective measures sufficient.

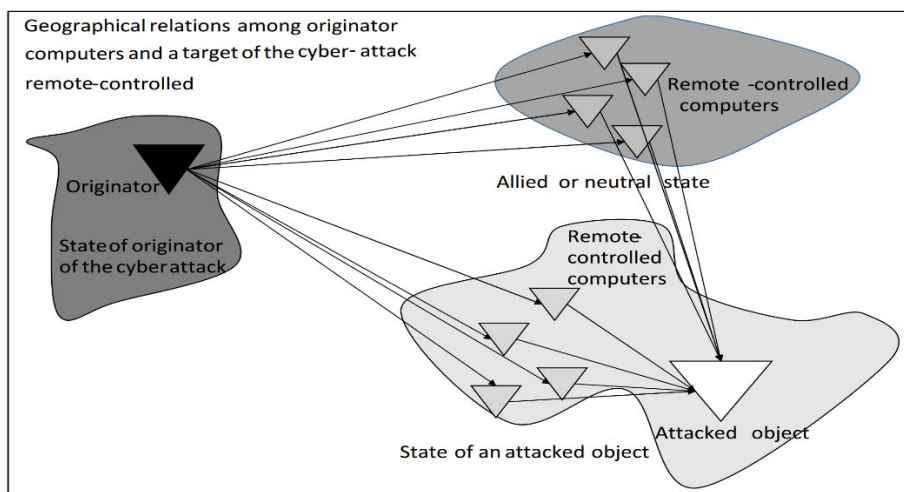


Figure no. 1: Example of territorial affiliation of an attacking organisation, used means and its targets

Using of weapons against a state organisation or a company registered on a territory of a concrete state or being important for this concrete state might be considered as a simple

criminal or perhaps as a terrorist act. This consideration is fully in responsibility of the concrete state, which territory or interest is targeted.

Considering the related situations also evokes a problem of terminology. When an armed conflict linked with the use of weapons is realised among non-state actors of the international arena treated as armed conflict or rather as a criminal or terrorist act? Similar problem with terminology comes from traditional definition of the weapons when the term weapon should include all means increasing human capabilities to limit interests of the opponent. In a case of cyber-attack should personal computers with their hardware and software used in cyber-attack be also treated as weapons with possible legal restrictions?

Similarly, as PMCs civilian commercial companies are also considered as a tool for economic pressure generation on the targeted state within the hybrid threat and hybrid warfare. Comparing to PMCs and their place in the fifth dimension mentioned by WEISSMANN's paper (Weissmann 2021, 65-67), commercial companies are quoted as a part of the second economic dimension.

In conclusion of this analytical part of the article, it is possible to formulate following findings:

Although PMCs are entirely new group of actors, their behaviour has been considerably changed. Today they act more overtly even they act directly in armed conflicts, often on behalf of concrete governments as a part of regular, state-controlled armed forces. Their members might face situations like soldiers of regular armed forces, e.g. captivity, but their status is not fully recognised by the present legislative framework. On the other hand, their members very often have problems with loyalty and obedience as well as with compliance of rules of armed conflict.

Concluding this analytical part, it is possible to formulate this finding:

Commercial non-state actors like international companies are many times much stronger from both economic and security point of view and they play much more important role within the international arena. They have monopoly in hardware and software for CIS worldwide and they are more active even in inner space. It is a question of time when interests of these commercial companies will cross with interest of concrete states or other similar companies. In this case simple conflict of interests may turn to an armed conflict where some or all sides will use available capabilities. HQ and facilities of these companies are located on a territory of a concrete state, which might be different from states engaged in conflict but attack against objects on its territory might be considered as a *casus belli*. Moreover, dismantling of management of the commercial company or destruction of their facilities may plunge some states or some economic sector worldwide into economic crisis.

3. Possible ways to solve present and expected future challenges regarding new actors of the international security environment

Based on findings and structure of the previous chapter this part of the article pays attention to possible ways how to solve discovered problems. At the beginning it is suitable to categorise sides of conflict with a use of weapons. There are recognised three possibilities of sides of a conflict and these combinations are listed in the table no. 1.

Since it might be unclear whether the term *armed conflict* is linked only to relations among states or about factions inside the state, in the table is used wording *conflict with a use of weapons* when a commercial organisation is involved. The term *state* also includes state owned organisations. The use of terms *crime* or *conflict with a use of weapons* depends on an angle of view – the commercial company engaged itself in the conflict does not recognise this situation as a *crime* but its opponent may see it otherwise, unless that organization is element

of the armed forces (Protocol Additional to the Geneva Conventions of 12 August 1949, Art. 43) of a party involved in the armed conflict.

Table no. 1: Possible combinations of conflicts among the state and commercial organisations

1 st actor	2 nd and other actors	Characteristics of the conflict
state	state	armed conflict
state	commercial organisation	crime or conflict with a use of weapons
commercial organisation	commercial organisation	crime or conflict with a use of weapons

In the second table, there is an example of the possible list of groups of actors potentially acting against their objects of interests.

Table no. 2: Categories of actors

Categories of actors engaged in potential hostile/criminal acts against other their objects of interests
States
Economically powerful International or national company/society owning advanced technology
Private security/military companies owned by a private person and controlled by a government
Private security/military companies owned and controlled by a private person
Criminal individual or a criminal group

Table no. 3 contains information regarding categories of activities of above-mentioned actors.

Table no. 3: Categories of activities of actors

Aim of activity	Category
to enrich members of the company	(organised) national or international crime
to spread terror to support political, religious, or ideological goals	terrorist act or (organised) crime, depending on an angle of view
to damage property or interests to kill personnel of the concurrent company	(organised) national or international crime
to damage property or interests to kill personnel of the concurrent/opposing state	war, armed conflict (organised) national or international crime

It is quite clear that the state should be fully responsible for any activities of all subjects using its territory in a cause of weak administration or/and lack of willingness to enforce effective legislation. Even in this situation it is questionable if it is a case of *casus belli* from other states in their effort to protect their interests or interests of organisations registered at their territories including their citizens. They are other tools of national or international policy included in abbreviation DIME (Diplomatic, Information, Military, Economic) when military tools should be really last resort.

In assistance to the states, there are international security organisations and their role should be increased to become effective and active when necessary because the time when commercial organisations would have approach to capabilities to act globally is not a question of whether but when and how. These international organisations should be able to support member states in their effort to enforce more precise and strict rules towards international and

national commercial companies acting on their territory. This is the only way to avoid crisis originating from their territory and at the end becoming a target for measures from side of other states and international society.

The military as the most powerful tool of national as well as international policy are many times the first responder in operations where PMCs are deployed. Military leaders, HQ, staffs at all levels in a chain of command have to be prepared to act effectively in an environment where partners like PMCs may disobey given orders, might commit war crimes or to change the side in according to an intent of their warlords. Despite of these challenges military leaders have to be able to explore all possibilities not just avoid any contacts with the PMCs of uncertain origin because there is a threat that the opposite side of the armed conflict might be able to use even this fluid possibility for its profit.

In order to conclude this chapter, it is possible to formulate following findings:

- The most important measure how to limit conflicts with the use of weapons and armed power, is a strong and continuous supervision of companies having capabilities to launch armed attack to enforce their interests. It means the main role should play the states where these commercial companies are registered and/or where these companies conduct their activities. This responsibility of the concrete state should be supervised by appropriate international security organisations and these organisations should be empowered to take effective measures towards states as well as towards commercial companies. International legal environment should be improved accordingly. Within states, their legislation should be improved to enable them effective surveillance of companies acting on their territory while keeping necessary freedom of their commercial activities not aimed against other subjects.

- Similarly, it seems it is naive there will be no PMCs in future therefore it is necessary to improve appropriate national as well as international legal frameworks for their existence and activities. States, where these PMCs are registered as any other commercial companies, should be able to supervise their activities and activities of their owners because at the end the state is responsible for any illegal acts of companies registered at its territory including compensation of related damages.

- Concerning participation of regular armed forces within operations, where above mentioned actors are active, HQs, and staffs of an appropriate level in a chain of command should be prepared to cooperate with these actors when necessary while still keeping in mind their potential volatility and uncertain status of their members. Existing plans of operations, including Rules of Engagement (RoE), Standing Operating Procedures (SOPs), should be improved accordingly. Education and pre-deployment preparation of military personnel have to be changed as well.

Conclusions

International and even global security has many dimensions but one of them, physical security of human individuals, their families is the most important. Societies including states and their interests against external attacks have still a higher position in the scale of values. Human society for this purpose have built up a complex system of habits, written and not-written rules and legal acts at national and international levels. Therefore, it is always the sensitive matter when this system has appeared imperfect or insufficient due to the development of a situation and one of consequences of this development is the appearance of new actors. Especially when these new actors are in many times more capable than traditional states.

The aim of this article, declared as highlighting these new actors, their specifics and possible consequences of their activities, should be reached since sorting out all connected legal issues is far beyond this short paper. It is then understandable that questions mentioned here are

formulated but awaiting appropriate answers, which should be delivered after extensive work of experts on international as well as national law. The attention of these experts should be oriented at least to international law, especially humanitarian law and law of armed conflict.

Aside of questions for legal experts, information contained in this article could be used for education at advanced studies of security experts at international level to present them the whole complexity of security situation and to show them a holistic approach to local as well as global security challenges. At national level, the article tries to stress the importance of careful and precise formulation of legal aspects of duties and rights for all companies registered at national territory in order to avoid any international tension due to their activities abroad.

In military domain, this paper should be explored for preparation of higher echelons national and international HQ and staff members in order to formulate appropriate rules of engagement and other parts of plans of operations and related directives and orders.

Recognising an approach to the future called “known unknowns”, generally we can expect even more actors having broader spectrum of interests as well as already known and even brand-new capabilities. Increasing number of actors will cause geometrically increasing number of their mutual interactions, which will be realised by new ways and means. Increasing number of interactions can probably lead to a number of conflicts and an ownership of capabilities to enforce their interests. When not paying enough attention to set up appropriate rules the unavoidable consequence of this situation is an increased probability of conflicts, even armed conflict between or better said among actors at international scene.

These challenges might be critical especially when existing and possible future technologies in wrong hands might cause serious international, even global problems, which this civilisation would not be able to solve. Complete cessation of all commercial activities in the field of security and defence or in advanced technology is not solution. In addition, hence initiative at any level leads this civilisation forward.

In this case a contemporary international legal system has faced in front of a complicated challenge hence it is necessary to define a role of PMCs and PSCs and legal positions of their employees during hostility in general, specifically in case of their rights in armed conflict in general and their status when captured. Similarly, it seems to be necessary to define a role of international society and its bodies in situations when international commercial companies are committing acts, which could be assessed as *casus belli* when they would be caused by states. Especially when their domestic states, states of their registration are not sufficiently strong to arrange rule of law.

At the very end, the final remark should be unfortunately that there are still more questions than clear, simple answers in this field.

BIBLIOGRAPHY:

- BAHGAT, Farah. 2021. “Syria: NGOs file torture case against Russian Wagner fighters.” *Deutsche Welle*, March 15, 2021. URL: <https://www.dw.com/en/syria-ngos-file-torture-case-against-russian-wagner-fighters/a-56873162>
- GlobalSecurity. 2021. “Wagner Group: Private Military Company ‘Wagner’.” Last modified July 30, 2021. URL: <https://www.globalsecurity.org/intell/world/russia/vagner.htm>
- Headquarters Department of the Army. 2015. Hybrid Threat Force Structure Organization Guide: TC 7-100.4. Washington, DC: Headquarters Department of the Army. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100x4.pdf
- HOLCOMB, Franklin. 2016. The Order of Battle of the Ukrainian Armed Forces: A Key Component in European Security. Washington, DC: Institute for the Study of War. URL:

- https://www.understandingwar.org/sites/default/files/ISW%20Ukrainian%20ORBAT%20Holcomb%202016_0.pdf
- KATZ, Brian, SETH G. Jones, Catrina DOXSEE, and Nicholas HARRINGTON. 2020. "Moscow's mercenary wars: The Expansion of Russian Private Military Companies." Center for Strategic and International Studies, September 2020. URL: <https://russianpmcs.csis.org>
- MILLER, Christian T. 2010. "Industry Talk: Contractor Deaths Accelerating In Afghanistan As They Outnumber Soldiers." *Feral Jundi*, April 14, 2010. URL: <http://feraljundi.com/1538/industry-talk-contractor-deaths-accelerating-in-afghanistan-as-they-outnumber-soldiers/>
- NATO Allied Command Transformation. 2017. Strategic Foresight Analysis: 2017 Report. Norfolk: Allied Command Transformation. URL: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf
- NATO. 2014. "Wales Summit Declaration." September 5, 2014. Last modified August 30, 2018. URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease
- Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.
- RAUENZAHN, Brianna; WANG, Jasmine; CHUNG, Jamison; JACOBS, Peter; KAUFMAN, Aaron and PUGH, Hannah. 2020. "Regulating Commercial Space Activity." *The Regulatory Review*, June 6, 2020. URL: <https://www.theregreview.org/2020/06/06/saturday-seminar-regulating-commercial-space-activity/>
- SCHWIKOWSKI, Martina, Mikhail BUSHUEV, Carole ASSIGNON, and Sandrine BLANCHARD. 2021. "Berlin and Paris concerned over Russian mercenaries in Mali." *Deutsche Welle*, September 16, 2021. URL: <https://www.dw.com/en/berlin-and-paris-concerned-over-russian-mercenaries-in-mali/a-59201331>
- WEISSMANN, Mikael. 2021. "Conceptualizing and countering hybrid threats and hybrid warfare." *Hybrid Warfare*, edited by Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm, 61-82. London: Bloomsbury Publishing. URL: <https://doi.org/10.5040/9781788317795.0011>