LUDOVIKA
UNIVERSITY PRESS

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE

Volume 22 (2023)
Issue 1

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

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

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

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

AARMS
ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE
Volume 22
Issue 1
2023

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

Publisher:

University of Public Service, Ludovika University Publishing House
Responsible for Publishing:
Gergely DELI Rector

Copy editor:

Zsuzsánna GERGELY

Typeset and print by the University of Public Service
ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

Contents

AARMS Vol. 22, No. 1 (2023) 5–21.

10.32565/aarms.2023.1.1

Special Vehicles and Equipment in Fire Operations Used in Different Regions[1]

Péter PÁNTYA[2]

Different parts of the world have different disasters or fire and technical rescue events. Economic, infrastructural and natural environmental differences cause great variances. The nations employ various organisations, depending on the available possibilities, with diverse technical solutions to eliminate the sources of fire, disaster, incident dangers. In case of fires and technical rescue occasions that have already occurred and require intervention and pose a direct threat to human life, physical integrity and property, these tasks are typically performed by fire brigade organisations. These organisations also carry out more or less extensive activities in their areas of responsibility; however, national solutions may involve the use of firefighting vehicles and equipment that differ significantly from one neighbouring country to another.

The article presents the general firefighting vehicles used internationally and in Hungary and their characteristic capabilities, together with the widely used technical equipment and devices worldwide, built-in or mobile firefighting machines. In this paper a wide-ranging inspection of firefighting vehicles are demonstrated, and the description of the firefighting equipment can be interpreted together with the carrier vehicles. By special fire engines, the author here means vehicles that are on standby in each country, but only in small numbers and only alerted a few times a year. An important aspect in this category is that the design and equipment of these firefighting vehicles are planned to eliminate special incident situations that are unlikely to occur, but pose a great threat to human life, physical integrity or the property of the country and citizens, even in the short term. The article focuses also on these less frequent, more specialised firefighting vehicles and technical devices, with a description of their typical deployment conditions.

When drawing the conclusions, the ideas and solutions found during the international outlook worthy of Hungarian adaptation are presented. Here the national adaptation possibilities of each international, special firefighting vehicle, the advantages they can provide and the expected disadvantages are examined. The content of the article is a general summary that fills a gap due to the small amount of international literature, which can also be used during research, investigation and education in this research field.

Keywords: *fire, fire operation, intervention, special firefighting vehicle, equipment*

[1] The work was implemented in the framework of project TKP2020-NKA-09, financed by the Thematic Excellence Program 2020 from the National Research Development and Innovation Fund.

[2] Assistant Professor, University of Public Service, e-mail: pantya.peter@uni-nke.hu

Introduction

Different disasters or fire and technical rescue events are happening all over the world. Economic, infrastructural and natural environmental differences cause great variances. Each nation engages different forms of organisation, depending on the available possibilities, with diverse technical solutions to eliminate the sources of danger. In case of fires and technical rescue occasions that have already occurred and require intervention, and pose a direct threat to human life, physical integrity and property, these tasks are typically performed by fire brigade organisations. These organisations also carry out more or less extensive activities in their areas of responsibility; however, in practice, national solutions may involve the use of firefighting vehicles and equipment that differ significantly from one neighbouring country to another.

In accordance with its title, the article presents the general firefighting vehicles used internationally and also in Hungary, and their characteristic capabilities, together with the widely used – also typical – technical equipment and devices worldwide, even built-in or mobile firefighting small–medium machines. A wide-ranging inspection of firefighting vehicles made and the description of the firefighting equipment can be interpreted together with the carrier vehicles. In the study, general fire vehicles include fire engines, water carriers, aerial apparatuses (ladders, platforms), but also mobile container carriers and cranes are presented. By special fire engines, the author here means vehicles that are on standby in each country, but only in small numbers and only alerted a few times a year. An important aspect in this category is that the design and equipment of these firefighting vehicles are planned to eliminate special situations that are unlikely to occur, but pose a great threat to human life, physical integrity or the property of the country and citizens, even in the short term.

The article focuses on these less frequent, more specialised fire vehicles and technical equipment and devices, with a description of their typical deployment conditions. The rationale for keeping them ready and deploying them will also be described. When drawing the final conclusions, the ideas and solutions found during the international outlook worthy of Hungarian adaptation are presented. Here, taking into account the geographical, road network and industrialisation conditions and economic opportunities in Hungary, the national adaptation possibilities of each international, special firefighting vehicle, the advantages they can provide and the expected disadvantages (e.g. maintenance, operation) are examined.

The article focuses mainly on traditional firefighting and technical rescue activities and the firefighting vehicles and equipment used. Due to the special needs and equipment of medical rescues, it is not discussed this time.

The present work is a niche work due to the very limited Hungarian and international literature. Its aim is to provide a brief description and characterisation of general and special internationally used firefighting vehicles, and to provide a broader background for further research in the field, also for non-mainstream firefighters and researchers. By drawing attention to the various specific vehicles and solutions, even among fire vehicles, future possibilities of national adaptations or development studies can be attached.

For space and editorial reasons, only a short textual and general description of the professional, national firefighting vehicles and equipment of the different countries is given, without illustrative pictures. For the specific reasons of the more specialised industrial fire brigade designs, which are adapted to local characteristics, there are still solutions that have not been considered here.

Methods

In preparing the article, a literature research was carried out in the Hungarian and mainly English language using public sources. In addition to a review of various journals or books, data found at and provided by different manufacturers were also used and researched. The available literature on the subject is rather scarce, so this article is intended to fill a gap.

The author also used his own experience gained in his firefighting profession, university teaching and research activities. Personal participation has been made through field research at recent international exhibitions in the last years, targeted consultations with industry experts in this field.

Results

The first thing to clarify is the basic purpose of the fire brigade and disaster management forces themselves. Typically, in most countries of the world, this is to save lives, carry out firefighting and technical rescue tasks.[3] In many countries, such as the United States of America or Germany, and in some cases Romania, the fire brigade is the basic health-related relief organisation, with the ambulances and medical equipment and supplies provided for this purpose. As it was delimited at the beginning of this article, this primary health rescue and ambulance service provided by the firefighting service area will not be examined in this work. Firefighting vessels of various sizes, boats and single-person watercraft used by fire brigades are not included in this article, nor are aircraft and equipment used for firefighting purposes.

The rescue of persons in immediate danger of their lives, various outdoor fires involving buildings or vehicles, or technical rescue operations in a variety of environments (road accidents, building damage) may require firefighting vehicles of various types to be on the scene of the incident.[4] In addition, there are a small number of incidents where the use of specific and specialised firefighting vehicles, which are also very different from ordinary fire vehicles, is justified.

[3] Goodenough 1978.
[4] Restás et al. 2018: 340–340.

General categories of firefighting vehicles

The fire engines

Typically, the basic firefighting vehicle in Hungary and in most countries of the world is the fire engine. There are also different sizes and designs of this category internationally; they are classified as light, medium and heavy (possibly with the designation small, medium, large). The difference between them lies in the size of the vehicle, the power of the engine, the power of the pump, the amount of extinguishing water–foam forming agent carried and, due to the physical differences in size, the amount and design of the portable firefighting equipment. As a practical example, in addition to the installed pumping equipment, the light–small category carries around 1,000 litres of extinguishing water, the medium category carries around 2,000 litres, and the heavy–large fire engine carries around 4,000 litres in Hungary, with a proportionately increased quantity of foam and other firefighting equipment. The advantage of the larger quantity of extinguishing agent and equipment available from larger vehicles is accompanied by the disadvantages of more difficult inner-city transport and mobility.

Within this category, there are also lightweight or pick-up versions intended primarily for small fire brigades and volunteer fire brigades. Compared to larger fire engines, there are solutions involving the pump, where removable, portable firefighting pumps provide the water stream as opposed to the built-in versions.

The basic purpose of the fire engines is to enable general firefighting operations to be carried out at a basic level, while also being able to transport the required number of firefighters. They carry breathing apparatuses and rescue bags, life-saving ropes, extinguishing water and fire extinguishers and their accessories, and various hand tools and small machines, as well as various other protective equipment and accessories for technical rescue. All of these are carried in a permanently ready and accessible state in the fire vehicle's cargo area, so that they are available at all times without the need to send out special equipment.

Other fire vehicles

In addition to fire engines, other general-purpose firefighting vehicles, which are relatively frequently alarmed to the scene of a fire, include:

- *The water carriers.* Their basic aim is to provide, transport and supply large quantities of firefighting water in water-scarce areas, even by shuttle. Thanks to their built-in pumps and the limited amount of firefighting equipment compared with the fire engines, they can even intervene independently, albeit to a limited extent. Their capacity for transporting personnel, i.e. intervening firefighters, is also limited, typically one to three personnel. The capacity to transport water can vary from around 6,000 litres up to 40,000 litres, depending on the country and the needs. This means that there are water transporters ranging from the heavy category to tractor-

trailer solutions, although the latter are limited in their applicability to long-distance transport of extinguishing water.

- *Aerial ladders, platforms.* These fire vehicles are basically on standby to rescue lives from different floors of higher buildings. In addition to this, they can also be used for water cannon firefighting from various angles from above during fires and for long-distance, even thermal imaging, reconnaissance and, in some versions, they can deploy their rescue platforms not only at height but also, to a limited extent, at depth – even under a bridge. They can be of either ladder or platform system design, these also affect their tactical usability in different incident scenes, environments.
- *The technical rescue vehicles.* Their primary tasks, as their name suggests, are to support the technical rescue fire activities, typically with technical equipment, and the typical staffing levels are accordingly reduced; in Europe typically one to two firefighters. Their design, similarly to that of fire engines, also includes light and heavy categories. The light category may be designated as 'rapid intervention' or 'road', as its role is to provide a basic primary technical rescue capability in the event of a road accident. On roads with higher traffic congestion, the smaller size helps the travelling and the deployment to the scene of the incident, but it is also considered more agile in terms of speed and acceleration. Due to the smaller cargo size, they are only able to carry basic, essential technical rescue equipment. Firefighting vehicles in the medium or heavy category naturally sacrifice these advantages in order to offer a wider range of equipment and the ability to carry larger sizes or numbers of items of rescue equipment. Some designs can provide additional lifting capabilities for the fire brigade with built-in or mounted rescue cranes, but with limited load capacity.
- *The firefighter crane trucks.* Their only task and ability is to lift and secure large, heavy objects during various fire and disaster management intervention activities. This can be lifting trucks or tractor-trailers in road accidents, but also craning damaged building elements. Apart from the fire brigade forces, only special crane vehicles from the construction industry or some associated services (e.g. the armed forces) are available for similar purposes.

Typical equipment carried by general firefighting vehicles

As described above, the fire engines carry the required number of firefighting personnel and the specialised machinery and equipment installed, as well as a variety of firefighting and disaster management equipment. These varied tools are available in the fire vehicles' cargo holds to support life-saving, firefighting and technical rescue tasks. These tools can be categorised according to several criteria. In one aspect, they may be manually or mechanically operated, but they can also be distinguished according to their purpose as firefighting, technical rescue, communication, and personal protection or other.

Briefly, the typical firefighting equipment supplied is as follows:

- Portable fire extinguishers of various sizes and extinguishing capacities, agents
- Hoses of various sizes and their fittings and tools
- Equipment for the supply of extinguishing water and the handling of hydrants

- Equipment for different types of fire extinguishing jets, ways (water, foam, powder)
- A variety of personal protective equipment such as breathing apparatus, boots, gloves, etc.
- Various hand tools, such as saws, shovels, axes, fire swatters
- Ladders ranging from small adjustable and folding ladders to larger extendable ladders
- Signalling, lighting and communication equipment such as traffic control devices, buoys, radios

A very important element is the variety of mechanical equipment that can be removed from the cargo holds by the firefighters and which can be used on the scene to assist fire operations. These can be chainsaws, hydraulic rescue – cutting equipment, disc cutters or generators.

Machinery and equipment installed in various fire vehicles

In addition to the obligatory elements, these vehicles are also equipped with blue lights and siren sound signalling and radio communication devices, as well as built-in normal/high pressure pumps, typically located in the rear behind the fire extinguishing water tank (with some exceptions, such as in the case of high-altitude rescue vehicles), but examples can also be seen mounted on the front of the vehicle or installed in the middle.

Other built-in equipment and devices include winches, work lights to illuminate the area – possibly floodlights, water cannons requiring manual operation and remote-controlled extinguishing streams, known as water monitors, extinguishers of various types, rigid or preassembled with a flat hose, quick-acting fire hoses, self-protection extinguishing systems and brass extinguishers. Less frequently, we can found extinguishing arms with occasional spikes, generators to support the vehicle itself and the intervention. There are also smaller cranes in less commonly seen built-in form and built-in compressed air tanks with quick-charging connectors for the on-site rapid charging of firefighters' personal breathing apparatus.

Modern versions of firefighting vehicles also have on-board computers, displays (monitors) and even printers to provide backup IT support during the firefighting operation or at the scene of the incident. In recent years, solutions based on removable and therefore portable tablets have been gaining ground.

Traditional multi-stage, normal and high-pressure pumps are commonly found in fire engines, with modified versions such as CAFS (Compressed Air Foam System), which requires a water-saving foam agent, and UHPS (Ultra High Pressure System) built-in extinguishing systems, which are also water-saving but effective for smaller vegetation or some indoor, road fires.

The specialised firefighting vehicles

In this section, a summary of fire brigade and disaster management vehicles with major differences compared to general use fire engines is presented. The differences are mainly related to the purpose and design of the vehicle. The more specialised and unique firefighting vehicles are designed to support and effectively perform only some fire and disaster management tasks, but their annual run is not significant. The following list shows the wide range of special fire vehicles in use internationally, but their use and the extent of use varies considerably from country to country.

For the purposes of this article, the following firefighting vehicles are classified in this category:

- *Container carrier fire trucks.* These containers kept on standby can be used for technical rescue, hazardous material handling, water purification, social support for firefighters (rest, food, hygiene, sanitation), fire extinguishing containers with built-in and mobile water cannons, various extinguishing agents (foam, extinguishing powder), flood protection, mobile control point or health – medical purposes. In practice, this list can never be exhaustive, a wide range of capabilities needed on the scene of a disaster can be easily implemented and deployed in containerised form. In this way, special capabilities can be alerted at any time and deployed to a given geographical area or site of incident in a short time (typically within one to three hours) to support the on-site activities of fire brigades and disaster management forces. The size of the containers themselves, and therefore the size of the transport vehicles required, varies from country to country and from task to task, with light and heavy duty versions generally available, but also examples of ultra-lightweight solutions.

Picture 1: A medium size container carrier fire truck in Italy

Source: Photo taken by the author, 2017.

- *General transport, loading, road maintenance, firefighting personnel and equipment vehicles.* These are basically similar to ordinary civil, industrial and commercial trucks, but with built-in blue lights, siren, markings, radio communication devices and the ability to be kept at the disposal of the vehicle by the emergency services at all times, to assist the fire brigade and disaster management organisations in their priority incident response activities. There are even different types of earth-moving equipment among the fire vehicles in some countries.
- *General command and administration vehicles.* Similarly to the above, a command or administrative vehicle differs only slightly from an ordinary vehicle, command vehicles may have additional equipment due to differences between countries and/or tasks. These could be, for example, the specialised firefighting equipment of the Hungarian disaster management operational service or the single command points and on-board terminals developed in other countries, specifically to support the on-site command activities of the specialised field.
- *Fire motorcycles and snowmobiles.* They are not commonly used, but in several countries (e.g. Germany, Spain, the United Kingdom) there are fast-moving fire motorcycles with the advantage of faster arrival, and thus faster on-scene reconnaissance and the start of the first intervention. Their disadvantage is the ability to transport only one firefighter with minimal special equipment. Snowmobiles are naturally used for the same purpose and with the same disadvantages, but only in certain countries where weather conditions warrant it.

Picture 2: Fire motorcycles in England

Source: Photo taken by the author 2017.

- *Airport fire engines.* There are several different types of designs, but it is important to note that the purpose of this article is to summarise general fire vehicle knowledge

and that the number of operations carried out by airport fire brigades is significantly smaller than the number of operations carried out by general, everyday fire brigade operations. For this reason, the typical airport fire engines are listed here under one paragraph. The basic requirement here is to be able to start and travel as quickly as possible, while transporting the typically very large quantities of extinguishing agents, so that in case of extinguishing airport fire engines the built-in pump must start operating the various extinguishing streams even while the vehicle is in motion, in order to ensure effective extinguishing. Since in the aviation world, the individual incidents involve the transport of large numbers of passengers and large quantities of goods in the presence of considerable quantities of hazardous materials and fuel. It is important to rely on own transported extinguishing agents, tactical support for firefighting by means of high reach extendable turret and piercing nozzle, monitors or carried high-performance fans, but also cooling self-protection of vehicles. The supplying of extinguishing water from hydrants and the resulting loss of time during the initial phase of the intervention would be an undue disadvantage, and the location and distance of the aircraft to be extinguished from the hydrants could be particularly significant, justifying a specific and large transport and extinguishing capability. Fires and technical rescues occurring in airport areas may take place outside asphalt and concrete surfaces, even at a distance of several kilometres, and these vehicles must therefore be able to meet the above requirements in a wide range of weather conditions (e.g. snowy–muddy ground).

Picture 3: An airport fire engine with working monitors

Source: Photo taken by the author, 2017.

- *Forest, wildland fire trucks.* Compared to general urban, road fires and technical rescue incidents in forest or agricultural environments, there are additional requirements for the fire vehicles. Forest fire trucks are basically similar to conventional and general fire vehicles, the difference being based on the specificities of the geographical areas

targeted and protected and the fires that occur there. In these geographical areas, in the open vegetation and forested environment, there are no good quality and adequate width of regularly maintained roads, fire hydrants. For this reason, solutions with good off-road capabilities, with the narrowest possible superstructure due to narrow and wooded roads and capable of transporting several firefighters are required, in addition to which water saving extinguishing methods (e.g. CAFS or UHPS) and the transport of their equipment (special hand tools and extinguishing equipment) are a priority.[5]

- *Reconnaissance, on-site mobile laboratories for fire brigades, disaster management.* The ability to detect the presence, exact substance and quantity of hazardous substances, known or unknown, but less frequently encountered, and the direction of spread, is not available to fire brigades in general fire operations, either by default or internationally. A rapid airborne analyser capable of detecting some typical gases (e.g. oxygen and carbon monoxide) is available in most countries on various fire engines, but needs that are more extensive can be met either in central laboratories or in mobilised, on-board versions designed for fire brigade and law enforcement purposes. In almost all countries, such specialised vehicle-mounted or transportable containerised solutions are available, providing rapid detection results at the scene of damage from different sources and in different forms (gaseous, liquid, solid powder), even in the fleet of several military or law enforcement agencies (e.g. police, defence, army).[6]
- *Vehicles handling the release of dangerous substances.* Diverse and specific equipment is needed to eliminate the immediate threat to the environment, human life and physical integrity posed by hazardous substances that have already been released. Incidents of this type are rare in comparison with general firefighting operations, but it is necessary to supplement general firefighting equipment and machinery in this respect. Such special equipment may include hoses, pumps or temporary storage containers resistant to various dangerous substances, but also special protective clothing and its accessories. These equipment and devices are kept in a vehicle or transportable container for easy and flexible alerting.
- *Mobile command vehicles.* The command of fire and disaster management incidents involving several fire brigades and associated services, affecting a large part of the population and covering a large geographical area, involves the difficulty of managing the intervention forces from several different organisations and the difficulty of maintaining visibility of the area. Additional levels of command and other support posts will need to be established on a temporary basis in relation to the direct command mode. The most common technical rescue or firefighting operations do not require such an apparatus and, importantly, do not require a major infrastructure. In case of different types of incidents, both command and control and the necessary support and administrative activities need to be carried out in a variety of external locations (e.g. out of town in winter and at night). Fire vehicles are essentially trucks, possibly passenger vehicles, with very limited office space (e.g. desk, keeping multiple documents on paper, briefing and tasking several participants simultaneously in a confined area, etc.).

[5] Wu et al. 2016: 174–184.
[6] Horváth et al. 2021: 110–125.

Mobile command vehicles can meet these needs as a minimum, either on vehicles of various sizes (from lightweight to extendable and semi-trailer versions) or in transportable swap-body container form.

- *Fire vehicles with a high degree of self-protection.* In an environment where particularly high or even varied hazards are present and intervention cannot be delayed, fire vehicles with a higher degree of self-protection can create safer conditions for both the vehicle and the firefighters on the move. Internationally, the number of such incidents is very low, while the cost of acquiring and operating fire vehicles designed for such an environment is high due to the small number of units and the special protection needs. Nevertheless, it is difficult to circumvent or replace their use by other means to achieve the objectives of the above-mentioned environments. They can be designed to provide protection against multiple hazards, such as explosions, thermal effects or hazardous substances of different types and composition.

Picture 4: An ultralight fire vehicle on duty in Slovakia

Source: Photo taken by the author, 2022.

- *Ultralight fire vehicles.* As there may be firefighting service interventions that require heavy-duty equipment, there may be a need for specially designed small fire vehicles for fire or disaster purposes in many areas. Such environments may include industrial, utility tunnels in the built environment or mountainous, heavily forested areas in the

natural environment. What they have in common is the scarcity of access roads, but fire interventions also require the transport of personnel, intervention forces and various specialised firefighting equipment, tools to the scene. For such purposes, depending on the environment, specially adapted (e.g. made to measure for tunnels) or modified versions of existing ordinary vehicles can be used, such as quads, ultralight flatbed or body-on-frame single or double four-wheelers. Ultralight fire vehicles can also be cab or open quads with rubber tyres and tracked, snowmobile versions, depending on the expected needs.

- *Remote-controlled special fire vehicles.* Over the last decade, there has been an increasing trend towards fully remote-controlled fire vehicles of various types and sizes or firefighting special purpose vehicles. These can be complex designs with dozer, knuckle or high reach extendable turret, pump and nozzles, water cannons, with near-vehicle suppressing capability, or special purpose solutions such as pressurised fans or mobile water cannons. They may also have limited towing capabilities and may be fitted with rubber or tracked undercarriages. They can also be deployed in marshy, near-water environments and in environments that pose a high load or hazard to humans, and range in size from the smaller half-metre to the size of a passenger car.

Picture 5: A remote controlled fire vehicle at an exhibition

Source: Photo taken by the author, 2022.

- *Tracked, special undercarriage fire brigade, disaster relief vehicles.* They can transport firefighting and other personnel, specialist equipment and intervention materials over extremely difficult terrain. In marshy, flooded natural environments, the more costly airborne capability, which provides only a short-term presence in the area, or the tracked and floating carrier vehicles mentioned here and found in several countries, which offer a more favourable alternative to the airborne solution, may be considered. This could also include firefighting with capabilities for use on tracks in a railroad environment or on private tracks in a winter mountainous environment, with similar size and intervention capabilities to those in general use.
- *Water, ice rescue, dive fire vehicles.* These fire vehicles are primarily for life-saving purposes from various forms of water (rivers and lakes, whether frozen surface or deeper bed) and from different forms of water. The purpose of the vehicles is to search and rescue persons who are in the water. The aim is to support the fire units by transporting specialised and protective equipment and built-in equipment, devices. In addition to rescuing persons, fire tasks include the search for, and possible recovery or support of various objects and vehicles in the water, but also special surface or underwater activities in case of various water structures, for example during flood protection. Fire vehicles providing water rescue capability typically consist of conventional light or medium-duty cargo vehicles with specialised cargo compartment design and possibly rubber dinghy towing or roof carrying capabilities.
- *Breathable air support vehicles.* Many fire tasks naturally take place in the presence of smoke, hazardous materials release or reduced oxygen levels, for example in the case of building fires. Respiratory protection of fire brigades is almost entirely provided by compressed air breathing apparatus, which requires the use of air cylinders that are already pre-filled and kept ready. These can provide 30 to 40 minutes of protection for the firefighter using them and, with the reserves carried by the fire engines, can support a one to two hour operation. In addition to the reserves held at fire stations, for prolonged and extensive incidents, it may be necessary to provide a larger stock on the scene of the incident, or even to provide a continuous solution for on-site refilling. These air support vehicles may be of a pallet or containerised design.
- *Rescue air cushion carrier.* Specially designed for specialised rescue operations from height, the specialised nature of these fire vehicles is almost exclusively in the rescue equipment they carry and its accessories. In practice, their design is achieved by providing a larger bale space and the basic equipment of a fire brigade emergency vehicle, even a light transport vehicle. The number of firefighters required to set up the bouncing cushion device is not transported by the vehicle, but by other fire vehicles.
- *Generator fire vehicles.* Vehicles designed to provide and support higher-powered electric power supply to incident sites or vital life safety or possibly medical – critical infrastructure buildings. As in some of the previous examples, their specialisation is limited to the provision of a single-purpose task, in this case by means of a light category carrier vehicle, trailer or containerised design. Apart from a trained driver, no additional operator firefighting staff are required.

- *Search dog fire vehicles.* Search for persons (under rubble or in forested–open areas), where search dogs can assist fire or other law enforcement forces, is also a life-saving activity within the scope of the fire brigade, disaster management. Among their tasks is the search for various materials or remains of materials at the scene to assist fire or police investigation. These fire transport vehicles are also mission-related, but they are not only used to transport the machinery, tools and protective equipment associated with the task, but also, and above all, to transport specially trained search dogs with special skills and the means to protect, care for and look after them.
- *Hose transport vehicles.* In several countries, vehicles carrying hoses of various types and sizes have been kept ready to support firefighting activities. These contain hoses specifically designed to provide firefighting water over long distances or in large quantities, possibly laid out and then recollected by their mechanised means when the stand-by is returned. Their use is not necessary for everyday fires, but for more serious incidents, their large size and volume make them necessary and larger, medium-heavy fire vehicles typically use them.

Picture 6: An impulse fire extinguishing fire vehicle at an exhibition

Source: Photo taken by the author, 2015.

- *Passenger buses, vans, trucks.* Both for general fire and disaster management tasks and for incidents requiring a larger number of personnel, it may be necessary to use vehicles for the transport of persons only. They can vary in design from light category to heavy category or large bus design, but are typically not equipped with special fire

brigade equipment and facilities other than basic radio communication, blue light, siren but examples of mobile command post capability can be seen.

- *Special, unique firefighting vehicles.* It may be used in relation to general firefighting activities where the vehicles and equipment available at conventional fire stations are not sufficient. The commonly available fire vehicles carry, to a limited extent, additional different extinguishing agents and solutions for their application on or in the firefighting vehicle. These special fire vehicles and the extinguishing agents they carry, such as foaming agents and extinguishing powders, are very rarely used for alarm and even less frequently for actual fire operations. The need to keep them on standby is more justified in an industrial environment, in or near a hazardous activity or plant, given that in such an environment the extent of a fire can be significant within a short time and can only be extinguished effectively and with less likely damage by special extinguishing agents. Typical extinguishing agents kept ready on board of the firefighting vehicles may include extinguishing powders, foam-forming agents, or certain extinguishing gases. There are also examples of water-based, but so-called impulse fire extinguishing vehicle-based solutions and turbine extinguishers with aircraft jet engines. The former can be used for small distances (a few metres) but for very short extinguishing times (a few seconds), while the latter can be used for longer extinguishing–cooling tasks, even over long distances of tens of metres, up to hours.[7]

Conclusions and discussion

The evolution of fire vehicles in the coming period

The changes in fire vehicles over the next few years will mainly be seen in the driven system. In several countries, and particularly in the more prominent, inner-city–industrial environments, we can see examples of the experimental use of all-electric driven in scattered locations in Germany, Spain or the U.K., as opposed to conventional diesel engines. It is expected that these will be developed in the near future, particularly in the area of battery capacity and fast charging. The main problem for electric fire vehicles is to keep the vehicle running for as long as possible, from start-up to the point of arrival at the scene, even at a remote location, and to keep it running for hours, taking into account the need to keep the energy-intensive installed equipment (e.g. pump) supplied. After the intervention, the vehicle must be able to return safely to the fire station, expecting that, while it is on the move, it may be alerted by another location with similar energy requirements. A further issue is the refuelling time to restore readiness, which for a diesel tank takes only minutes, which is still difficult to keep up with current capabilities.

There is also a slight change and evolution in the transported, portable firefighting equipment, with the petrol engine equipment being replaced steadily, at international level, by battery-powered, electric driven machinery. These firefighting appliances can

[7] Wallington 2004; Dermek 2011.

be easily replaced in the cargo holds of existing fire vehicles, and modernisation can be carried out within a day.

With the increasing mobility of battery-powered small appliances for firefighting purposes, less attention is being paid to the issue of fire engines as a power source. Nevertheless, in this section of the article, the author draws attention to the possibility of this, i.e. the availability of an on-board generator power capability and compressed air system. The power source they provide can be used within a limited distance from the fire engine, but within a few metres to ten metres with an electrical extension cord or air hose.

Keeping maintenance and operating costs for the firefighting service low will continue to be a priority in the near future. This can also be achieved by solutions that can perform as many functions as possible in one vehicle, i.e. a single fire engine design should be sufficient to meet the needs of firefighters in widely differing fire and technical rescue situations.

The range of equipment for remote-controlled fire vehicles and appliances is expected to continue to expand, as will their capabilities, with increasingly high-quality standard and thermal imaging cameras, greater extinguishing capacity, and more firefighting, other equipment systems both integrated and installed.[8]

The next step forward is the training of drivers of fire vehicles

Virtual training, including the development of near realistic driving and pump or other equipment handling simulation-training tools in fire vehicles, as well as software simulation training using virtual augmented reality, are becoming increasingly popular. Even hybrid target solutions are available today, such as the control of the pump only on a wall panel with monitors or projected surfaces, or the creation of a realistic driver's cab with visual displays or projectors. These solutions are expected to become more realistic and to be developed for an increasing number of devices, with more detailed digital virtual representations as the IT back-end develops.

For reasons of space and editing, this article only gives a general description of the various firefighting vehicles and equipment, but it is planned to expand on the various sub-areas which could be particularly useful in the field of education or for a real primary introduction to the field.

References

Dermek, Milan (2011): *Hasicské automobily na Slovensku.* Zilina, Slovakia.

Goodenough, Simon (1978): *Fire! The Story of the Fire Engine.* New York: Chartwell Books.

Horváth, Hermina – Kátai-Urbán, Lajos – Vass, Gyula (2021): Transportation of Flammable Dangerous Goods in Hungary. *Védelem Tudomány,* 4(4), 110–125.

[8] Suslavičius–Bogdevičius 2003: 89–96; Sivakumar et al. 2020.

Restás, Ágoston – Pántya, Péter – Rácz, Sándor – Érces, Gergő – Hesz, József – Bodnár, László (2018): A megelőző és mentő tűzvédelem valamint az iparbiztonság kapcsolódásai. In Vass, Gyula – Mógor, Judit – Kovács, Gábor – Dobor, József – Horváth, Hermina (eds.): *Katasztrófavédelem 2018: Veszélyes tevékenységek biztonsága.* Budapest: NDG DM. 340–340.

Sivakumar, A. – Babu Sekar, Jagadeesh – Vignesh, Sathya – Muthukumar, Shyam – Yogapriya, J. (2020): Autonomous Standalone Fire Engine with LIDAR-ROS. European *Journal of Molecular and Clinical Medicine*, 7(4).

Suslavičius, Vladimiras – Bogdevičius, Marijonas (2003): Improvement of Technical Parameters of Fire Vehicles and Equipment. *Transport*, 18(2), 89–96. Online: https://doi.org/10.3846/16483840.2003.10414072

Wallington, Neil (2004): *The World Encyclopedia of Fire Engines and Firefighting.* London: Annes Publishing.

Wu, Chengxuan – Zheng, Yanping – Wang, Zhe (2016): Design of a Multifunctional Forest Fire Vehicle. *Open Journal of Transportation Technologies*, 5(6), 174–184. Online: https://doi.org/10.12677/OJTT.2016.56022

AARMS Vol. 22, No. 1 (2023) 23–32.

10.32565/aarms.2023.1.2

Networks Enabling the Alliance's Command and Control

Attila GULYÁS[1]

The Alliance's wide area networks enabling operational command and control (C2) are under continuous revision in order to facilitate the wide spectrum data exchange between NATO Command Structure (NCS), NATO Force Structure (NFS) elements and other key organisations.

The focus is – as always – on the information technology's researches and network-enabled capability development.

It is clear that running the current NATO wide area network has challenges in terms of network management, information security and counter-cyber operations. Therefore, it requires a viable transformation to a wide area network with a higher-level resiliency and scalability.

Having supported by NATO Communications and Information Agency (NCIA), the decade's one of the most important tasks is to re-new, re-design and re-organise the existing classified network domain in support of efficient C2 for the current and future operations.

In this scientific article, I will provide with a short historical background of NCIA's efforts in creation of a more resilient classified domain-net and the needs of core and functional services within the Alliance to introduce the already decided, the viable solution of classified network enhancements.

Keywords: *infocommunications networking, CIS, command and control (C2)*

Introduction

The North Atlantic Treaty Organization (NATO) General Communications and Information Systems (CIS) network (NGCS) was introduced in 1997 in support of NATO Command Structure (NCS) elements (e.g. Supreme Allied Command Transformation SACT, Supreme Headquarters Allied Powers Europe SHAPE, Joint Force Command Brunssum JFCBS, Joint Force Command Naples JFCNP etc.) in the unclassified and classified security domains. In connections with that National Defence Networks (NDNs) and NATO Force Structure (NFS) elements were also required for the interconnections in the abovementioned physical and logical domains in order to provide with the highest level possible multi-connectivity between NATO and national commands. This common

[1] Colonel/OF-5, Director CIS/IT HUN General Staff, e-mail: attila.gulyas@mil.hu

aim has required the establishment of a comprehensive, overarching network structure called NGCS.

The NFS elements have organic support units dedicated for the all-level-support including CIS; however, the NCS principal commands might have no nationally dedicated support units for this purpose. Consequently, this is one of the needs of the establishment of an organisation, which provides the maximum level CIS support in the unclassified and classified, the static domains of CIS networking for NCS and NFS. To accomplish the tasks, the NATO Consultation, Command and Control Agency (NC3A) was formed in 1996[2] embracing the SHAPE Technical Centre (STC) in The Hague, Netherlands and the NATO Communications and Information Systems Agency (NACISA) in Brussels, Belgium. NC3A was part of the NATO Consultation, Command and Control Organization (NC3O) and reported to the NATO Consultation, Command and Control Board (NC3B). In July 2012, re-structuring the NC3A the NATO Communications and Information Agency (NCIA) was established.[3]

One of the key premises of the freshly formed NC3A (later NCIA) was to establish the NATO Core Network (NCN) enmeshing the NCS, NFS and NDN elements connected in the physical domain through gateways, routers and firewalls. In this term, the NC3A has begun to be the organisation embracing both NCS and NFS CIS elements into one comprehensive and scalable network in the unclassified and classified static domains.[4]

NATO Network Enabled Capability (NNEC) initiative promoted the use of NATO classified domain as operational consultation, planning and execution tool across the Alliance providing top-down approach from the principal commands down to national enclaves; meanwhile, the NATO expansions of the late 1990s (Hungary joined NATO in 1999) required new ways for network extensions both in philosophy and materiel.[5] The Connected Forces Initiative (CFI) established the notion of zero-day-connectivity, making that a strategic priority for the freshly joined, connected countries.[6] Zero-day-connectivity enables freshly joined and already existing Alliance members to run core CIS services plus selected basic functional services in order to provide the principal C2 functions with a coherent fundamental networking even before any exercises and operations launch.

Interoperability requires overarching connectivity in terms of Core Enterprise Services (CESs) such as telephony, e-mailing, video-teleconferencing and chat plus selected Community of Interests (CoIs) provided by NCIA primarily, listed in the NCIA Costed Services Catalogue and Service Rates.[7]

NFS and later the Joint Command and Control (C2) Capability (JC2C) initiative led the nations to create NATO Readiness Forces (NRFs) with the need of interconnections into the NGCS. This endeavour turned to high-scale connections towards Multinational

---

2 Károly 2013: 18–21.
3 NCIA official website.
4 NCIA official website (for more information see www.ncia.nato.int/about-us/newsroom/a-history-of-nato-support.html).
5 NATO NNEC website.
6 NATO CFI website.
7 NCIA Costed Services Catalogue.

Headquarters following the NATO Readiness Action Plan (RAP),[8] which further cemented the NATO classified domain as one of the foundation pillars of the Alliance's high readiness forces through enabling effective C2 from top to down commands (from strategic to tactical level).

NC3A, then NCIA is to cope with these challenges, has generated mesh networking in the classified domain utilising Mons and Evere in Belgium, Lago Patria (Naples) in Italy as services and data centres/hubs for NATO Enterprise (CES and CoIs) services. Most nations deliver their Information Exchange Requirements (IERs) as priority by simply extending the NGCS down to the national HQs. This means a stovepipe connectivity from the abovementioned data centres run by NCIA down to national HQ (users) challenging the information channels/lines of communications with a broad diversity of threats, requiring scalable measures to guarantee cybersecurity, overall.

Another relevant topic is the finance of Alliance-wide CIS in terms of the common funding/separated (national) funding. Alliance members pay budget to the NATO funds but based on surveys and experiences the rapid expansion of the Alliance, accelerating from the first decade of the 21st century shows that 80% of the actual NGCS footprint was left outside the NATO common-funded capability packages. This means that freshly joined nations were/are not eager to or capable of the improvement of their classified C2-enabling CIS following the NCIA-proposed renewal cycle of hardware and software commonly used in NATO. These results a vast amount of obsolete and cyber-related vulnerable equipment and tools within a mesh networking still designed not to compartmentalise these national extensions. Nowadays, when the cyber challenges are the most demanding threats in our world interconnected, these have been weakening and might compromise the entire NGCS. It is worth noting that the proliferation of nationally managed classified information services' domains, which were designed to individually synchronise their directories (e.g. file servers) and e-mailing (e.g. exchange servers) with the NCIA Automated Information Systems (AIS) domains, the NCIA Enterprise is an indispensable hub for the organisations to communicate with each other.[9]

Therefore, it seems obvious that the currently NCIA-managed NGCS at least the static classified network's domain needs to be revised and re-designed as an important task to give immediate answers to the 21st century's cyber challenges. The relevant counter measures leave great portions of decisions in the hands of organisations (HQs, nations, etc.) to promote their measured, tailored but at least minimum level appropriate actions within the creation of their own network and services.

After this short introduction, this article is to review the ongoing NATO procedures in order to find solutions to the continuous development of network-enabled requirements (Information Exchange Requirements IERs), incorporating the nations and other organisations as information hubs into an Alliance-wide network with embedded and real networking capabilities.

In this article, I will provide with the short descriptions of current researches/trends from NCIA to nations in creation of a resilient wide area network in the classified domain

8 NATO RAP website.
9 NCIA/AFS/2021/050501 – AFS Joining Instructions. 3.

and I will describe the expected steps from nations and other organisations to achieve this higher level of interconnected network of networks.

A viable solution

It is apparent that the Alliance's principal commands (NCS elements) must be supported by NCIA in the future as well. Revolutionary changes can be achieved in the fields of NFS and other organisations' Information Technology (IT) networks, utilising the Federated Mission Networking (FMN spirals)[10] model as a schema in joining the NATO classified static networks. The aim is to create a kind of classified Internet within this relevant domain, giving chance to the nations and organisations through their dedicated host nation and support units to manage their own networking, initially with the heavy support of NCIA.

A possible answer to the emerging challenges is the NCIA initiative Alliance Federated Services (AFS) project. The NCIA has organised the kick off/pilot conference on this topic in April 2019, which was based on the Alliance's Polaris[11] programme. Polaris is a modernisation initiative embracing almost all segments of NATO developments, in order to create an Alliance characterised by cutting age technology within the communications area, scoping on the IT, to provide with resistant and resilient CIS networking, forging the Alliance to comply with the 21st century's challenges. One of the important segments of Polaris is the CIS/IT modernisation led by NCIA, as stated by NATO documentations C-M(2015)0041-REV2 (national/organisations' PoPs), PO(2014)0801 (CIS Security), C-M(2017)0062 (NATO C&I Vision).[12] Surveys and experiences identified that more than 600 Point of Presences (PoPs) exist within the NATO umbrella enmeshing the entire classified static network. To reduce the numbers of NCIA-managed PoPs and involve more the nations and organisations into their management, there is a need to re-design, upgrade/install and manage/maintain as a maximum 2 PoPs per entities, run/supervised commonly by NATO (NCIA) and nations/organisations. Through these PoPs, the entities can utilise the CES and CoIs by NCIA, also they have possibilities to design, operate and maintain their own services (federated services), also to lend or borrow them to/from other NATO nations/organisations (NCIA Business to Business model). It is supported by NCIA migrated services in terms of CES and CoIs utilising cloud services very well-known from the civilian, the private IT environment.[13] The NGCS must transform to a more up-to-date, modern IT network, also it will change the name to NATO Communications Infrastructure (NCI).

[10] Low 2021.
[11] NCIA official website: *Polaris programme*.
[12] Trouvé 2021.
[13] NCIA/AFS/2021/050501 – AFS Joining Instructions. 8–9.

The way to the optimum

Based on the FMN[14] concept,[15] the new AFS model must utilise the following layers' federations (in accordance with C3 taxonomy[16]).

- Network layer
- Core (enterprise) services layer
- Cybersecurity layer
- Information Technology Infrastructure Library (ITIL) layer
- CoI layer
- Verification and validation layer

Once the NNG interconnections completed thus the layering, the layers' federations might be the key for success. After defining the federated layers, it is worthwhile to deep-dive into the levels of network layer in order to overview then identify the real needs and tasks to nations, organisations to re-set their connectivities. In Table 1 are to be found the pre-planned federation initiatives focusing on the network layer.

Table 1: Federation initiatives

Type	Definition	Explanation
Type 0	Currently NGCS PoPs	Might be transformed to NCI node
Type 1	CoIs extensions mostly for NCS	For a specific organisation/need/ requirement; planned to be guided and supervised by NCIA only
Type 2	This layer is for NFS, HQs and other organisations	N/A
Type 3	Alliance and national C2 elements without direct NCIA supervision	N/A
Type 4	All which are not in the abovementioned levels and are not supervised by NCIA	N/A

Source: NCIA AFS Conference report 248-4/4/2019/NATO as of 02 April 2019.

The target of this modernisation effort is to bring the focus to Types 2–3–4, designing a new network layout, exchanging the hardware (PoPs), re-design the Internet Protocol (IP, currently IPv4) addresses, develop the Service Management (SM) including Quality of Service (QoS) measures.

Therefore, it appears obvious that join AFS first and foremost must be a national effort for all Alliance member organisations (NCS, NFC) and other HQs, national extensions. It also seems evident that the highest profits and benefits will be at the national or organisation level with this re-structuring once they have their state-of-the-art, newly constructed network extensions with the bright possibility of further enlarging, with the re-organisation of CES and CoIs to other Alliance members, organisations.

---

14 Károly 2020: 571–586.
15 NATO SACT Future Mission Network (FMN) Concept FCX 0010/TT-8523/Ser: NU, October 2012.
16 Károly–Németh 2019: 55–67.

Design principles

As I have already flagged out the current NNG (border router with border protection services BPS) will connect directly to the organisation, nation's border router. The NNG can be commonly managed by NCIA and the respective nation; however, the management of national gateway (e.g. edge routers) and BPS must be the role and responsibility for the nation. In other words, boundary protection mechanism (can be local and/or centralised) will be placed by the respective nation.[17]

Also, border protection measures are the clear interest of each nation. Figure 1 shows the possible solution depicted the current network situation forward to the near future visions.

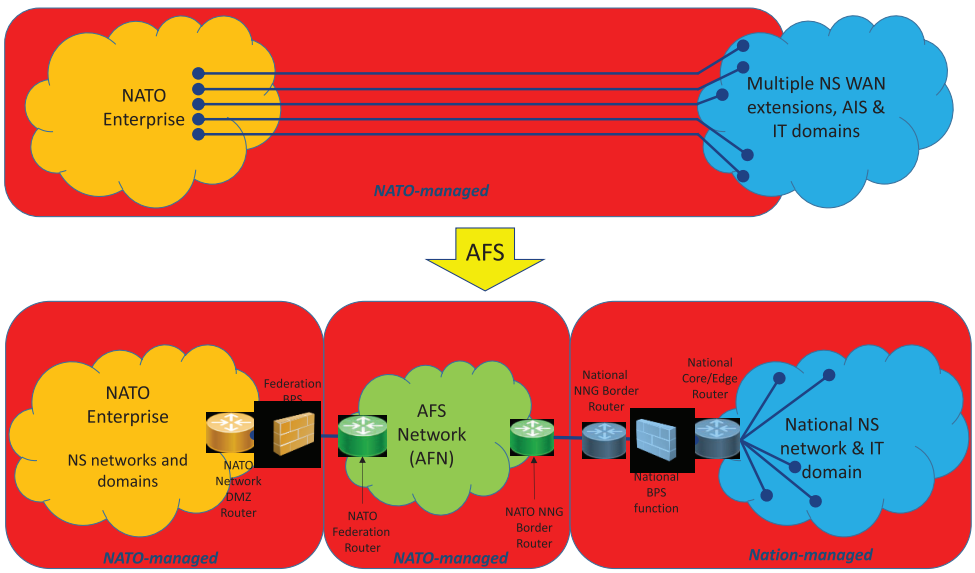

Figure 1: Current and future static networking environment

Source: Defourneaux 2021

Figure 1 clears that the new networking allows the Alliance to operate in the entire network as classified Internet (IP routing and Domain Name Services DNS) with the essence of the national efforts for building blocks of it. National networks might have, might receive services from NATO Enterprise; however, each of them are highly encouraged to develop their own Alliance Federated Networking (AFN) capabilities in terms of Core Enterprise and functional (CoIs) services brokered by/with/under direct support and supervision of the NCIA, who still governs the entire NATO classified static networking.

[17] NCIA/AFS/2021/050501 – AFS Joining Instructions. 7.

NCIA will also support the national IPv4 private space allocations, establishing the NCIA Naming and Registration Authority (NRA).[18] It is recognised that during the last decades NCIA and nations/organisations have less care of proper IP-spacing and like in the civilian environment, as demands require, the IPv4 must be exchanged to IPv6, the migration of the IP-spaces[19] is inevitable and vital in building a cyber-resilient classified network.

Road to success

The NCIA has designed the steps of any organisation to re-transform their obsolete network to federated static networking.[20] As I have stated already, this is an NCIA-led initiative therefore, the Agency offers viable steps to achieve the full connectivity. Here are the most important, the required actions by any nation, organisation as follows in Table 2.

Table 2: Steps for federation

Steps	Actions
Step 01	Upon invitation by the respective nation or organisation, NCIA gets a common view of the NS extensions, IT services (DNS, Email and Directory) and IP space.
Step 02	The nation, organisation has the decision, which extensions are to migrate and which ones would remain end-to-end managed.
Step 03	The nation, organisation and the NCIA NRA agree on the final delegated IP space available for the entity to manage.
Step 04	The nation, organisation takes over and uplifts the legacy assets (gateways, routers, BPS) used for the migrated extensions, where required.
Step 05	The nation, organisation or NCIA commissions the NNG and national NNG Edge Routers.
Step 06	The nation, organisation aggregates connections or networks behind the national NNG Border Router (this is national responsibility), then develop and maintain the IT services.
Step 07	The nation, organisation provides security accreditation for this freshly formed network, including the elements inherited from the legacy extensions.
Step 08	NCIA migrates the national NNG Border Router connection from the legacy NGCS router to the NATO NNG Border Router.

Source: Compiled by the author based on NCIA/AFS/2021/050501 – AFS Joining Instructions. 16–17.

Having accomplished the steps above, obviously the nations and organisations' benefits would be that the respected entity has the full control and management of her entire classified static network with the possibility of future extensions including enlarging the current classified static web with deployable (mission) networks or elements implemented in a coherent and scalable, resilient way. That is the vital point when static and deployable classified networks – utilising the FMN compliant networking principles – shall be

[18] NCIA/AFS/2021/050501 – AFS Joining Instructions. 8.
[19] Murdock 2021.
[20] Friedrich–Janinez 2021.

federated in terms of layers then CES and CoIs.[21] All this means that this freshly formed cloud would be outside the NATO Enterprise footprint; therefore, it has the full individual management of IP space assigned to it by NCIA NRA. Nations and organisations can create new network nodes, change the network topology (extend or reduce) and upgrade network appliances as well as deploy new applications and services. In another approach, this federated method gives the nations, organisations free hands to run their classified network business as they wish, more importantly as the operational requirements, changings enforce.

Summary, conclusions and the way ahead

As it apparent, the currently used NGCS cannot be managed any more due to specific reasons defined by NATO strategic and operational documentations. There is a need for transformation, there is a requirement of urgent network upgrade utilising the FMN principles in the NATO classified, static networking as well. NCIA has initiated the AFS project in 2019 to answer the challenges of the 21st century clearly identifying the needs then setting the rules, roles and responsibilities by NCIA itself, NCS, NFS and other elements, especially nations and organisations how to re-design that obsolete classified static networking currently called NGCS.

NCIA provides the comprehensive Joint Membership and Exit Instructions (JMEI) as well, to any entities across the Alliance to read, digest, utilise and finally act for the maximum effort. That is the evident account of the network transition initiative, following the steps guided by that document, nations, organisations can achieve their successful and rapid joining into this freshly defined and formed networking.

Hungary has also stepped forward on this way establishing the core network planning team of our classified static networking. At this phase, this board's primary task is to review the current HUN NATO S*cret Network's (HUN NSN) layout and nodes, PoPs than create an upgrading plan, a viable solution with the proper timeline to the decision makers, how and when, most importantly with whom can the HUN NSN be transformed first, then federated with, in accordance with AFS principles.

The challenge is given now. I strongly believe, soon HUN NSN shall turn into a new classified network organised in accordance with AFS principles.

List of abbreviations

AFS	Alliance Federated Services
BPS	Border Protection Services
C2	Command and Control
CES	Core Enterprise Services
CIS	Communications and Information System

[21] Athanasiadis 2022.

CFI	Connected Forces Initiative
CoIs	Community of Interests
DNS	Domain Name Services
FMN	Federated Mission Networking
ITIL	Information Technology Infrastructure Library
JC2C	Joint C2 Capability
JFCBS	Joint Force Command Brunssum
JFCNP	Joint Force Command Naples
NACISA	NATO Communications and Information Systems Agency
NC3A	NATO Consultation, Command and Control Agency
NATO	North Atlantic Treaty Organization
NCI	NATO Core / Communications Infrastructure
NCIA	NATO Communications and Information Agency
NCS	NATO Command Structure
NDN	National Defence Network
NGCS	General Communications and Information Systems (CIS) network
NFS	NATO Force Structure
NNG	NATO and Nation Gateway
PoP	Point of Presence
RAP	NATO Readiness Action Plan
SACT	Supreme Allied Command Transformation
SHAPE	Supreme Headquarters Allied Powers Europe

References

Athanasiadis, Christos (2022): *Transition of MND-C to AFS as a Nation AFS and NNG Update.* Brussels: NCIA HQ, NCIA – HQ MND-C workshop, SME presentation, slide No. 13.

Defourneaux, Gilles (2021): *AFS Joining Instructions Who? Why? What? How?* AFS workshop. Brussels: NCIA HQ.

Friedrich, Gernot – Janinez, Deflet (2021): *Alliance Interoperability Architecture Federated Mission Networking, and Alliance Federation Services.* AFS workshop. Brussels: NCIA HQ.

Károly, Krisztián (2013): Szövetséges erők követése az afganisztáni hadszíntéren. *Honvédségi Szemle*, 141(3), 18–21.

Károly, Krisztián (2020): Automatizált erőkövetési képesség megvalósításának lehetőségei a Magyar Honvédség híradó-informatikai rendszerében. In Pohl, Árpád (ed.): *Biztonság és honvédelem. Fenntartható biztonság és társadalmi környezet tanulmányok II.* Budapest: Ludovika Egyetemi Kiadó. 571–586.

Károly, Krisztián – Németh, András (2019): The Possibilities of Supporting the Public Functions with Fleet and Force Tracking Systems. *AARMS*, 18(3), 55–67. Online: https://doi.org/10.32565/aarms.2019.3.5

Low, Warren (2021): *Protect Core Networking – Workshop Introduction/Context.* Brussels: NCIA HQ.

Murdock, Aidan (2021): *IP Addressing.* AFS workshop. Brussels: NCIA HQ.

NATO CFI website. Online: www.nato.int/cps/en/natohq/topics_84112.htm
NATO NNEC website. Online: www.nato.int/cps/en/natohq/topics_54644.htm
NATO RAP website. Online: www.nato.int/cps/en/natohq/topics_119353.htm
NCIA/AFS/2021/050501 – AFS Joining Instructions.
NCIA Costed Services Catalogue. Online: https://dnbl.ncia.nato.int/Pages/ServiceCatalogue/Services.aspx
NCIA official website. Online: www.ncia.nato.int/
NCIA official website: *Polaris programme.* Online: www.ncia.nato.int/what-we-do/nato-consultation-command-networks/polaris-programme.html
Trouvé, Pascal (2021): *AFS Contribution to Polaris programme.* AFS workshop. Brussels: NCIA HQ.

AARMS Vol. 22, No. 1 (2023) 33–49.

10.32565/aarms.2023.1.3

International Criminal Cooperation in the Shadow of the Coronavirus Pandemic[1]

Ivett CSONTOS-NAGY[2]

European cooperation in criminal matters is a priority in all EU Member States, whether in the detection, investigation or judicial fields. In recent years, I have been carrying out research in the field of organised crime, during which I have realised that in investigations involving two or more Member States, it is almost impossible to achieve the desired objective without criminal cooperation. Then, in the spring of 2020, investigative authorities had to deal with a variable such as the coronavirus pandemic, one of the consequences of which was that personal contact was minimised. However, one of the most important factors for successful and effective police cooperation are personal contacts, which can be achieved through training, meetings or even personal exchanges of views during the course of a criminal case.

However, the activity of organised crime groups is ongoing, although it is fair to say that they favour cyberspace, but they have not given much thought to overcoming the obstacles that arose during the coronavirus pandemic. They have emerged in e-commerce, online marketplaces, but at the same time, they have expanded their existing network of recruiters and started to think globally. Their distribution activities and logistics have also changed. Typically, the online space can be observed for criminal activities such as drug trafficking, arms trafficking or fraud.

The pandemic has also reduced the effectiveness of international cooperation on crime. In the research for this study, I am looking for answers to the question: what tools and methods of cooperation were available to the investigating authorities in the period before the pandemic and could they be further expanded? I will then contrast this period with the escalated situation during the pandemic. My research questions will include how and to what extent the coronavirus pandemic affected international criminal cooperation, in particular the use of Joint Investigation Teams. I also shed light on the question: what are the opportunities and obstacles to the use of available tools for criminal cooperation in the case of crimes committed in the online space?

The threat is growing, it has more and more international aspects, so I think there is a need for deeper cooperation, not only between law enforcement agencies,

[1] The project TKP2020-NKA-09 was completed with the support of the National Research Development and Innovation Fund and financed by the Thematic Excellence Program 2020.

[2] E-mail: Nagy.Ivett@uni-nke.hu

but also involving the private sector and civil society. It is important to make the citizens of all countries aware of the threats they face.

Keywords: *international criminal cooperation, coronavirus, cyberspace, cooperation tools*

Introduction

In the context of international cooperation on crime, countries have realised that one of the essential elements in the fight against organised crime is to work together in a cooperative way. This has led to the creation of European Union agencies, such as Europol, which bring together the Member States of the European Union. All this was preceded by the emergence of the issue of globalisation at the end of the 20th century, as János Sallai points out in one of his studies, "the Earth has shrunk into a global village".[3] This period was followed by the idea of a Europe without borders in 1985. Border controls were physically abolished with the accession to the Schengen area, creating an area without internal border controls.[4] Not only did this allow the free movement of capital and labour, but it also allowed the free movement of people, one of the consequences of which was that crime was transformed, no longer physically borderless. In short, these factors, among others, have led to the need for more effective joint action by the countries involved in organised crime.

In my research into the field of organised crime, I have realised that there are several factors that influence its development and that it has several consequences. International cooperation in criminal matters includes instruments that can make it possible to bring all members of a criminal organisation to justice. I approach my research from the crime detection and law enforcement side, from the perspective of investigative authorities, i.e. international police cooperation, and prosecution, i.e. international judicial cooperation, with a specific focus on European criminal cooperation. However, police cooperation and judicial cooperation are not the same thing, there are similarities and differences, but they both fall under the concept of international criminal cooperation. Both areas of cooperation will be touched upon in this study.

The paper will synthesise the international criminal cooperation tools used by investigating authorities and prosecutors, in the period before and during the pandemic, and will examine whether these tools can be further expanded. The research question is whether and to what extent has the coronavirus pandemic influenced international police and judicial cooperation and, if so, how? I will limit my research to the Joint Investigation Team as an available tool that offers an excellent opportunity for cooperation between several European Union Member States.

---

3 Sallai 2015: 135.
4 European Commission s. a.: 4.

I will also examine whether the pandemic has had an observable impact on the work of the Joint Investigation Team. Since the impact of the coronavirus has shifted crime to the online space, I have also asked the research question on cybercrime: what tools are available for detection that enable international criminal cooperation and are there any obstacles to cooperation? The study was helped by the spontaneous interviews conducted during the research (looking at both prosecutors and police officers perspectives), through which I plan to conduct more in-depth research on the topic in the future. In order to understand the basics of international cooperation in criminal matters, I believe it is necessary to take a historical perspective, including the distant past of international cooperation in the fight against crime.

Review of international cooperation in criminal matters

Throughout history, organised crime networks have adapted to the times, and police and judicial authorities of all ages have responded. There has been much research, both at home and abroad, into the roots of international criminal cooperation, but for the purposes of this paper I think it is important to look back to the early days.

The first signs of international crime can be traced back to the industrial revolution, when the creation of industrial plants and the need to earn a better living led to people moving to cities. The first law enforcement journal of 1869 reported the arrest in Vienna of a Romanian man who had seduced several young girls to satisfy his lusts, which already shows the rise of international crime in Europe at that time.[5] With the emergence of trafficking in girls, several bilateral agreements were concluded between neighbouring countries in the late 19th century and early 20th century, followed by an international agreement signed by several countries in Europe, including Hungary.[6] It was recognised that closer work and coordination between countries would help in the fight against crime. In 1911, the journal *Közbiztonság* [Public Security], a journal of police theory, published the term internationally organised crime, which was the most modern type of international criminal. "The public danger of this international organization is manifested not merely in the large extent of its area of operation, but chiefly in the fact that the perpetrator and victim are mostly from different countries. This is what makes the success of the investigation so difficult."[7] Subsequently, in 1911, at the German Police Conference in 1912, principles were laid down for seeking an international convention to allow police authorities to communicate directly with each other for apprehending individuals suspected of important police matters and other serious crimes. The first International Criminal Police Congress took place in Monaco in April 1914, and was attended by delegates from Hungary. One of the issues discussed at the Congress was the establishment of an international bureau for the registration of criminals.[8] It was at this congress, that the idea of the future Interpol

5 *Közbiztonság*, 22 August 1869. 1.
6 Sallai–Borszéki 2022: 985.
7 *Közbiztonság*, 23 April 1911. no. 17. 222.
8 Dorning 1937.

was born, with 300 advisers from 24 countries attending. However, the First World War put an end to further action.[9]

The 19th century also saw the emergence of extradition, mutual legal assistance and the transfer of criminal proceedings, but it was not until after the Second World War that we can speak of real international cooperation in criminal matters. Bilateral treaties continued to be in force and then efforts were made to institutionalise criminal cooperation. It is interesting to note that criminal cooperation is the youngest area in the history of European integration. One of the results of this institutionalisation was the Trevi Group, which was set up in 1976 to combat terrorism, to promote closer police cooperation and to combat drug trafficking.

Also relevant to this study are the Schengen Agreement of 1985 and the Convention Implementing the Schengen Agreement, which entered into force in 1995. It will be explained later that cross-border operations are still being carried out under the Schengen Agreement, so that the provisions on police cooperation contained therein are still in force today. The landmark date following the Schengen Agreement was the entry into force of the Maastricht Treaty on 1 November 1993, which led to the creation of the European Union. Within the European Union, the Treaty of Amsterdam, which amended the Maastricht Treaty, and the Treaty of Lisbon, which entered into force on 1 December 2009, extended the role of national parliaments and the European Parliament. It has become necessary to harmonise the laws of the countries within the European Union and to unify national legal systems. Finally, institutions were created at European Union level to facilitate, among other things, cooperation in criminal matters. Noteworthy are the creation of OLAF (European Anti-Fraud Office) and Eurojust.

In Hungary's case, the possibility of criminal cooperation was for a long time limited to extradition, but this changed with the country's accession to the European Union.[10]

Forms of international criminal cooperation and law enforcement agencies

The study presents possible platforms that can be used to fight serious and organised crime. In particular, the cooperation tools used by investigating authorities in the detection phase will be presented. In order to understand the forms of international cooperation in criminal matters, it is essential to understand the legal basis and the legal background, and to note that currently international cooperation in criminal matters is characterised by horizontal cooperation, which means that states assist each other in proceedings that involve an international element.

One of the classic forms of criminal cooperation is extradition, which is still relevant today in relation to third countries. The principle of mutual recognition has also been transposed into criminal cooperation, the idea of which was first mooted in 1998, based on the recognition by the countries of the European Union of the enforceability and

[9] Sallai–Borszéki 2022: 988.
[10] Páhi 2019: 59–60.

validity of each other's acts.[11] This is also linked to the Tampere (1999–2004), The Hague (2004–2009) and Stockholm (2010–2014) Programmes, which also focused on the fight against organised crime and terrorism within the European Union. EMPACT (European Multidisciplinary Platform against Criminal Threats) is linked to international cooperation in criminal matters and has become a centralised process of cooperation as defined by the above programmes. The EMPACT policy cycle develops pro-active actions to achieve pre-defined objectives, coordinates action against serious and organised crime, takes into account the involvement of third countries in crime developments, and thus cooperates with bodies outside the European Union.[12] For example, in the 2014–2017 policy cycle, priority crimes included reducing heroin and cocaine trafficking, reducing cybercrime, combating trafficking in human beings.[13] The police and judicial authorities of the Member States also have an important role to play in the fight against serious and organised crime and in achieving the objectives set, which common police and judicial cooperation between Member States can make even more effective.

As regards the legal instruments involving international cooperation in criminal matters, there are the instruments of non-judicial cooperation, the rules on the validity of foreign convictions and international mutual legal assistance in criminal matters. The legal instruments of non-judicial assistance type cooperation can be found in Act LIV of 2002 on the International Cooperation of Law Enforcement Agencies.[14] Accordingly, the forms of cooperation may include:

- direct exchange of information
- exchange of information with a law enforcement body of a Member State of the European Union
- the establishment of a Joint Investigation Team
- the use of a person cooperating with a law enforcement agency
- the use of an undercover agent
- cross-border surveillance
- hot pursuit
- the use of a liaison officer
- covert intelligence gathering on the basis of international cooperation
- cooperation with the special intervention unit of a Member State of the European Union[15]

The rules on the validity of foreign convictions are not relevant to the research, but international mutual legal assistance is of particular importance for organised crime, even when the aim is to reach law enforcement authorities in third countries. In response to inter-state needs, a uniform legal framework for international mutual legal assistance in criminal matters has been developed at the legislative level, which is enshrined in Act XXXVIII of 1996 on International Mutual Legal Assistance in Criminal Matters.

11 Csákó 2016.
12 Kolozsi 2022: 283.
13 Hegyaljai 2014: 128.
14 Páhi 2019: 61.
15 Act LIV of 2002 on the International Cooperation of Law Enforcement Agencies 8. § (1).

International mutual assistance in criminal matters is carried out by judicial authorities through requests between themselves. The forms of international mutual legal assistance in criminal matters are as follows:

"a) extradition,
b) transfer of criminal proceedings,
c) acceptance and surrender of the enforcement of sentences of imprisonment and measures involving deprivation of liberty,
d) acceptance and surrender of the enforcement of confiscation or forfeiture, or of a penalty or measure having equivalent effect (henceforth: confiscation or forfeiture),
e) acceptance and surrender of the enforcement of irreversibly rendering electronic data inaccessible, or of a penalty or measure having equivalent effect (henceforth: irreversibly rendering electronic data inaccessible)
f) procedural legal assistance,
g) laying of information before a foreign state."[16]

In the framework of criminal judicial cooperation, the aim was to establish a single system for taking evidence, which would help to create a single investigation system in the European Union. Therefore, the issue of the European Investigation Order is also closely related to this topic, the domestic legislative background is contained in Act CLXXX of 2012 on Cooperation with the Member States of the European Union in Criminal Matters.[17] It was set up to enable the lawful acquisition of evidence in cases of cross-border crime, thus speeding up investigations. This will allow evidence to be obtained in the course of the investigation of criminal organisations, even with covert means, as it is possible to use covert means within the framework of a European Investigation Order.

In the context of the European Investigation Order, I would mention controlled delivery (because controlled delivery can be requested) as a diagonal cooperation of international criminal cooperation, which requires close cooperation between police and judicial authorities. During the spontaneous interviews, police officers stated that controlled transport is frequently used. Controlled transport is not specifically mentioned in Act XC of 2017 on the Hungarian Prosecution Code, but the prosecution's position is that it may fall within the scope of covert surveillance and that requests for it from another Member State are also made in the context of judicial cooperation and thus serve the purpose of evidence. I note here that if a Member State concerned does not cooperate in a controlled transfer, the whole thing may fail, despite the approval of the other Member States.

Among the forms of international cooperation in criminal matters, I would also mention the implementation of cross-border covert surveillance, which can be an important form of cooperation in dismantling criminal organisations. The Rapid Response and Special Police Services are authorised to carry out this task, as are the staff of the National Tax and Customs Administration. They are used when the border of Hungary is likely to be

[16] European Judicial Network s. a.
[17] Based on the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

crossed or when the act under surveillance does not constitute a crime in itself, based on Article 40 of the Convention Implementing the Schengen Agreement. If, on the other hand, it is foreseeable that the act itself will constitute a criminal offence, but covert surveillance is used in the meantime, covert surveillance must be carried out because of the legal framework for international mutual legal assistance in criminal matters for controlled deliveries.[18]

The following is a brief description of the law enforcement agencies that can be linked to the international criminal cooperation instruments used in practice.

Interpol

The idea of the creation of Interpol (International Criminal Police Organization) has already been mentioned above, in the context of the first International Criminal Police Congress in 1914. Hungary was also a founding member in 1923 in Vienna, when the international organisation known as Interpol was established. Interpol has 195 members around the world, all of which aim to work together to make the world a safer place. As a global organisation, it can provide platforms for cooperation. In Hungary, the National Police Headquarters, International Law Enforcement Cooperation Centre, Interpol's National Central Bureau is currently designated as a cooperation channel to Interpol, so Hungary has direct access to various Interpol databases, such as the DNA database, the child sexual exploitation image database, the personal database.[19]

Europol

Europol (Central European Criminal Investigation Office) is a fully-funded EU agency, which started operations on 1 July 1999 in The Hague, the Netherlands, and is one of the most important institutions for police cooperation. Europol's tasks and objectives are to support law enforcement authorities within the European Union, to facilitate criminal cooperation, to make cooperation smooth and to ensure that information and criminal intelligence flow as quickly and safely as possible between Member States. A number of platforms are provided by Europol to facilitate these objectives and can be used by law enforcement agencies of the Member States. For example, the EIS (Europol Information System), which is a criminal database available in the official languages of the Member States and can identify possible overlaps between investigations. In addition, the SIENA (Secure Information Exchange Network Application) system ensures the flow of information and rapid communication, i.e. criminal intelligence. For these systems, endpoints have been set up in the Member States, there are several endpoints within a given country, but in Hungary, for example, it is also possible to contact the Member States through

[18] Nyeste 2020: 833.
[19] Nyeste 2020: 843–844.

the National Police Headquarters, International Law Enforcement Cooperation Centre to obtain information.[20]

Eurojust

Since its creation, one of the main objectives of the European Union Agency has been to coordinate investigations carried out by the Member States within the European Union. Its tasks include facilitating the fight against serious and organised cross-border crime and linking the law enforcement authorities and prosecutors of the Member States. It coordinates the judicial response of the prosecution services or investigating authorities of the Member States. Eurojust's activities focus primarily on organised crime groups. However, it can also provide operational assistance for cross-border operations, as it operates 24 hours a day, 7 days a week. It also provides support in official translations and manages parallel investigations. It can set up and fund a Joint Investigation Team or organise a Joint Action Day. Of particular importance for organised crime is the possibility to seize the assets of members of a criminal organisation. It also provides links to more than 50 jurisdictions and manages cooperation with third countries.[21]

SELEC

The SELEC (Southeast European Law Enforcement Center) is an important international organisation, especially from Hungary's point of view, as non-EU member states are also members of the SELEC, with whom cooperation is essential due to their geographical proximity, as the SELEC also has 11 member states and 25 partner countries in Southeastern Europe. The aim of the SELEC member countries is to combat cross-border organised crime through police and customs. It provides law enforcement authorities in Southeast Europe with, for example, a venue for operational meetings, regional operations and a platform for information exchange. Like Europol, the SELEC has liaison officers who are delegates from each Member State. Under SELEC, the Southeast European Prosecutors Advisory Group (SEEPAG) promotes judicial cooperation and operates in a way that prosecutors can exchange information in the investigation of cross-border crimes.[22]

International Law Enforcement Cooperation Centre

A brief introduction to the International Law Enforcement Cooperation Centre is important, as it is the only body that institutionalises international criminal cooperation in Hungary and has jurisdiction throughout the country. It functions as a kind of information channel

[20] Nyeste 2020: 834–835.
[21] Eurojust s. a.
[22] Southeast European Law Enforcement Center s. a.

between the investigative authorities within the country and the authorities abroad, whether in the European Union or in third countries. It was established on 1 February 2000 under the aegis of the National Police Headquarters. It cooperates with Europol and Interpol. In connection with the International Law Enforcement Cooperation Centre, I should also mention the Europol Hungarian Liaison Office, to which the Hungarian law enforcement agencies delegate a member, so that they can represent Hungary directly, in person, at the Europol headquarters in The Hague, and this personal presence will allow for an even faster flow of information.

The pandemic and international cooperation on crime

During the pandemic, organised crime groups responded to the situation shortly after the outbreak in spring 2020. They sought to map the market as soon as possible, identifying the segments that may or may not have been affected by the pandemic. However, there was uncertainty on the part of the investigative authorities, for example, in the domestic context, a large proportion of criminal investigation staff were assigned to quarantine and other tasks related to the pandemic, thus criminal work was sidelined. During this period, the most common crimes in Europe included cyberattacks, grandchild fraud, other frauds, phishing, the looting of health institutions and pharmacies.[23] Organised crime groups also realised that many citizens had lost their jobs and therefore had no income, so they took advantage of this to start recruiting people into criminal organisations. These criminal organisations also became increasingly violent. This is why we can say that the impact of Covid-19 was quickly felt by law enforcement agencies and required a swift response from law enforcement.

A report published by Europol in 2020 already provides data on how certain areas of crime have been shaped by the epidemic. In case of cybercrime, for example, perpetrators have been at the forefront of how to take advantage of the situation. We have seen first-hand how staying at home and working from home made people vulnerable at first. Individuals may have experienced symptoms of anxiety. The perpetrators also exploited fears about the epidemic and relied on people's insecurity.[24] Something else to note here is that victims in the real space immediately feel the effects of the attacks on them, but in the online space they do not feel that a crime has been committed against them.[25]

As the internet became the platform through which communication took place and goods and food were purchased, the threat became even greater and cyberattacks and online fraud were seen to increase. To give an example, there have also been changes in the drug trade, shipments have not stopped, they have continued to arrive at distribution points in Europe, onward movement from distribution points may have been a barrier due to physical border controls. Exports of chemical substances and precursors from China have decreased, so the production of drugs has not been assured. However, it can be seen

[23] European Council s. a.
[24] Dornfeld 2020: 193–204.
[25] Z. Nagy 2021.

that whatever the criminal organisations were up to, the aim was always to make a profit, or even the highest possible profit, even during the pandemic.[26]

It is the literature reviewed and the spontaneous interviews conducted by the investigating authority and the prosecution prior to the study that form the practical basis of the research. It is not by chance that the issue of the pandemic arose at the beginning of the research, as it has had an impact on crime itself, and I thought it worthwhile to address whether there were any barriers to international criminal cooperation. From the answers I received, it became clear that international criminal cooperation was also influenced by the coronavirus, for example the quarantine of postal parcels. According to the answers given by the investigative and prosecutorial staff, the pandemic initially had a major impact on criminal cooperation, which led to a sudden halt. It became less influential after a few months. It is interesting to note, however, that while one might think that the impact was negative, the interviewees also found that the pandemic had positive benefits in addition to the negative ones, but this will be discussed later.

It was emphasised during the interviews, both from a police and prosecutorial point of view, that the lack of personal relationships became a negative factor. Suddenly rules were imposed on everyone, so that, for example, attending an operational meeting or even face-to-face meetings within a given country were difficult to implement. Nor was face-to-face presence possible during the implementation of international criminal legal assistance. Since face-to-face meetings had to be minimised for both prosecutors and investigating authorities, meetings and exchanges of information obtained were also moved to the online space. Solutions such as Zoom, Microsoft Teams or Skype meetings were developed to enable communication in both police cooperation and judicial cooperation. Nevertheless, there have also been examples of cooperation partners travelling despite restrictions because a particular case warranted it.

In the period before the pandemic and in the period after spring 2020, the potential platforms for international criminal cooperation did not change according to the research results, but the use of the above-mentioned communication channels should be highlighted, meaning that before spring 2020, online communication channels were less used as potential platforms for criminal cooperation.

The use of the Joint Investigation Team

One of the aims of international criminal cooperation is to ensure that the information obtained can be used as evidence as the investigation progresses, during the prosecution and trial phases. There are also instruments which in themselves guarantee this, such as the Joint Investigation Team, which is the best example of cooperation between police and judicial authorities.

The reason why it is the Joint Investigation Team (JIT) that I am referring to in particular is that it is a complex form of procedure in the detection of criminal organisations in which all the necessary elements are combined, for example, international criminal

[26] Europol 2020: 7–9.

cooperation in criminal proceedings takes place, on the one hand between the Member States participating in the JIT, and on the other hand between the prosecution and the investigating authorities. But let us look at some statistics: after 2010, the number of JITs started to increase, with hundreds of cases reported annually. Hungary participated in JITs for the first time in 2011, and in 2017 there were twelve JITs.

In more detail, the aim of establishing JITs is to centralise those criminal cases that require complex investigative and prosecutorial work, which is costly for the Member State concerned.[27] Act CLXXX of 2012 on Cooperation with the Member States of the European Union in Criminal Matters regulates the conditions for the establishment of a JIT in Hungary. Among other things, it specifies in which cases it can be established and when the crime is considered to involve several Member States.

Europol and Eurojust assist the JIT. With Europol's support, an operational meeting should take place, with the provision of a location, before the Member States agree to set up a JIT. Europol's role is important because information is exchanged through it before and during the setting up of the JIT. Eurojust is involved in the organisation and, if necessary, financial support of the JIT.

Another argument in favour of Member States often working within a JIT to dismantle a criminal organisation is that direct communication is ensured, exchange of experience is possible, face-to-face meetings are easier to organise and evidence is obtained through legal channels and under supervision. Related to Article 70/C § (4): "In the course of the operation of the Joint Investigation Team, in accordance with the agreement, the means of evidence or procedural steps taken by a member of the Joint Investigation Team, whether Hungarian or a member state, in Hungary or a member state, shall be deemed to have been taken as if they had been taken within the framework of the procedural assistance for the purpose of obtaining or providing the means of evidence or taking the procedural steps."[28] Within the JIT, covert means may be used or information obtained by covert means may be transmitted via the SIENA channel, as may the unauthorised sending of scanned copies of interrogation reports.

The use of JITs has been deeply affected by the pandemic. On the prosecution side, it was reported that in 2020, there were spectacularly fewer JITs initiated by investigating authorities, and that those that were in progress were extended. There was also a lack of face-to-face meetings within JITs and delegated members were not able to be present at procedural actions carried out by other cooperating Member States, but other means of information exchange were used, such as online meetings, communication through the SIENA channel. Following the sudden stop and the lifting of the restrictions, more and more JITs were formed, Member States tried to carry out procedural acts within the country until then, and then agreements were concluded with the Member States also involved in the same offence.

During interviews with members of the investigating authorities, it was mentioned that, in addition to the SIENA channel, another communication platform for the rapid

---

27 Szijártó 2019.

28 Act CLXXX of 2012 on Cooperation with the Member States of the European Union in Criminal Matters 70/C. § (4).

flow of information has also been developed by Europol called VCP (Virtual Command Post), which is a downloadable application for phones, similar to Viber or WhatsApp, and is called "WhatsApp for Law Enforcement Officers". It is secured by a username and password and the exchange of data is encrypted, which requires only a mobile phone, thus allowing real-time exchange of information. In my literature search, I read about another useful criminal cooperation tool that was developed for post-terrorist attacks and the response to them, Quick Response for Operational Centers (QROC), a platform that also provides real-time information exchange. In addition, another solution developed by Europol in 2016 is the Operational Real-Time Collaboration Solution (ORTICoS), which allows information to flow quickly and securely during joint operations via mobile phone.[29] These applications are well adapted in practice, with developments showing that while SIENA is only available to different teams and networks, they can be accessed via their own mobile phone with a username and password. They can also be used within JITs and, in fact, at the time of the Covid-19, applications via the phone were a particularly popular communication channel.

The prosecutors mentioned a network within the JIT to help find solutions to technical difficulties in cooperation. One such difficulty is the secure exchange of large amounts of data files. The European Commission has proposed the creation of this specific platform, which would further aim to enable participants to communicate easily and securely with each other and to coordinate the day-to-day activities of the JIT between the participating countries. An additional advantage of the platform is that shared evidence can be better tracked and, if a third country requests information, the participants can be immediately aware of the sharing with that country.[30] A so-called JIT exchange platform has been developed, which can even include video conferencing, chat facilities, file uploading and downloading. The uploaded files can be seen by the other parties in the same way, so if they need them, they can just download them from there, like a Google Drive folder, which can be accessed by whoever has access to it and can download the files they need.

JIT therefore has many advantages from a judicial and police cooperation perspective. To summarise, the advantage is that the parties conducting parallel investigations can quickly share the operational information generated and evidence is already exchanged, which is important from a forensic point of view. This means that if it is foreseeable that several requests for mutual legal assistance or European investigation orders would be issued, it is more appropriate to set up a JIT. There are more things to consider, if it is already foreseeable that it will be necessary to question witnesses or suspects abroad, it is also easier to carry out investigative acts through a JIT. However, there can be obstacles to JIT, such as lack of language skills, costs, administration, but these obstacles can be avoided if they are identified early and are already included in the JIT agreement.

[29] Monroy 2020.
[30] European Commission 2021b.

Criminal cooperation tools for crimes committed in the online space

People's lives have become easier since the Internet came into being, our daily lives have become faster and the flow of information has become more complete. Criminals have noticed this and the investigating authorities have had to react.[31]

Investigations in cyberspace also face a number of challenges. Invisibility, latency, sophisticated procedures all make the job more difficult. It is interesting to note that in case of crimes committed in the online space, organised crime in the classical sense is not always present, but one-man offenders can also make large profits by exploiting the vulnerable and gullible nature of others. As already mentioned, cyberspace has become a growing crime scene because of the coronavirus. This was the compelling reason why in this paper I will also discuss in a few sentences the other possibilities for criminal cooperation when talking about cybercrime. It should be noted that, at an organisational level, there are also many efforts within the European Union to support investigations in cyberspace by various means, and there are a number of conventions governing cooperation between Member States. All the international bodies discussed above contribute to providing some support.

During the interviews with the prosecutors, I received the answer that all available cooperation tools can be used, but beyond that there is one possibility based on a convention that is more than twenty years old, but the reference to this in practice, is not very common. This is the Council of Europe's Convention on Cybercrime (Budapest Convention, opened for signature in Budapest, in November 2001), which was promulgated in Hungary by Act LXXIX of 2004. After the interview, while studying the Budapest Convention, I discovered that already in 2001 new trends and new ways of committing computer crimes appeared. We can also read in it that the Member States are trying to combat the new phenomena with as much effort as possible, but that the efforts to be effective and efficient vary from one Member State to another. One important element of the Budapest Convention was data retention, for which practical and legal solutions had to be found. At that time, there was an increase in various forms of sexual abuse of children, which is why investigating authorities were forced to obtain evidence through some form of cooperation. One of the aims of data retention is that the Member State concerned by the request should ensure that the data are stored and possibly backed up for the requesting party. During the interview, I was also made aware that the Second Additional Protocol to the Budapest Convention has been drafted, which countries can sign from 12 May 2022. As cybercrimes are on the rise, so is the electronic data generated in the online space, so it would be justified to use digital data as evidence. It is the Second Additional Protocol that tries to fix them in the framework of international criminal cooperation. It includes, as an innovation, "procedures to strengthen direct cooperation with service providers and entities in the territory of the Member States, such as requests for information on domain name registration (Article 6), the transfer of subscriber data (Article 7) or the enforcement of requests for the rapid

[31] I. Nagy 2021: 109.

production of subscriber and traffic data (Article 8)".[32] According to the addendum, the accelerated disclosure of stored computer data in an emergency, the accelerated transfer of stored personal data and the knowledge and transfer of digital content are also covered. In this context, it was suggested during the interview with the prosecutor that, if possible, the Budapest Convention and its Second Additional Protocol should be "promoted" among investigating authorities, as more should be done to ensure the use of digital data as evidence.[33] It was noted that the United States of America is also included in the Budapest Convention, which is important because most service providers are based in the United States of America, so it would be important to have smooth cooperation, but requests from Facebook and other service providers also occasionally run into obstacles.[34]

Another important cooperation possibility that was mentioned during the interview with the prosecutors, which specifically promotes judicial cooperation, is the European Judicial Cybercrime Network (EJCN), which was established in 2016. It aims to assist investigations that focus on crimes committed in cyberspace. It also aims to improve the efficiency of prosecution and ensure a wide range of evidence. In addition, it acts as a communication channel, if a face-to-face meeting is to take place, Eurojust hosts the meeting. Major conferences are organised as an opportunity for countries to exchange experiences, learn from each other's legal systems and examine case studies. The EJCN is working to establish a legal framework that can regulate cybercrime at international level. At the prosecutorial level, there are also major obstacles to accessing data stored in cloud storage, and cooperation with service providers does not work smoothly in their case.[35] During the interview with the prosecutors, it was also discussed that each member state has a specialist (prosecutor) who communicates with other member states through the EJCN when international contact is needed in the investigation of a cybercrime, whether it is police or judicial cooperation. It is therefore important that investigating authorities communicate and seek assistance from prosecutors, as such a cooperation tool may be the key to fully investigate a cybercrime.

Summary

In conclusion, it can be concluded from the answers given during the interviews, for both parties, that there is no need to further expand the available cooperation tools and methods, there is no reason to expand them, the technical, technological and legal tools are available, but if all investigating authorities and prosecutors' offices would also be brave enough to use the tools they have less experience with, they would also help in the fight against organised crime. It is important to note that around 95% of cooperation takes place within the European Union, but organised crime, especially cybercrime, often requires cooperation with other third countries (see the United States of America).

---

32 Szomora 2022.
33 European Commission 2021a.
34 European Council 2019.
35 European Union Agency for Criminal Justice Cooperation s. a.

In terms of the basis for international cooperation in criminal matters, both from the police and the judiciary, it is clear that a great deal of emphasis is placed on personal contacts built up over the years, but in the case of our country this network of contacts seems to be increasingly lost due to turnover in the police forces, making it more difficult for foreign counterparts to engage in a more direct, personal relationship. When asked what the obstacles to cooperation are in some cases, it was told that the person himself is the biggest obstacle to international criminal cooperation, and that paper-based administration within a country, but also with other countries, takes more time, but that the positive effect of the Covid-19 is emphasised in this respect.

I have noted above that the coronavirus has not only had negative consequences. According to interviewees, online consultations, which initially seemed cumbersome, made communication and information exchange much more flexible and faster. The digitisation and rapid access to documents was also a positive outcome, for example in the case of sealed instruments with a prosecutor's or judge's authorisation. Although, in the domestic context, paper-based licensing is still the current practice. There were also examples of those who previously would not accept documents on paper only now having to accept them via email in response to the virus.

According to most interviewees, the future goal should be to continue to exploit online, digital platforms in international criminal cooperation and to promote further digitisation. It would be feasible if all agencies with organised crime at least had the means to conduct a video conference on or near their own computers. Another suggestion from the prosecution side was that it is up to the perception of the managers of the investigating authorities to be able to take effective action against organised crime, i.e. to organise the staff appropriately for the task. In a case where there is an international link to the criminal organisation, but the rapporteur does not have a deep knowledge of the possibilities of cooperation platforms, he should be assisted by someone who is experienced in this field, for example, who has attended a Europol hospitality, i.e. it is a question of work organisation. But to be self-critical, the same applies to the prosecutors' offices, because not all prosecutors are excellent when it comes to organised crime.

Finally, I would like to mention one innovative thing that was mentioned in the interview with the prosecutors and that could make the fight against organised crime even more efficient and effective in the near future. This is the digitisation of the European Investigation Order, an exchange platform that is already being piloted but is not yet official. The platform consists of an online interface (which will be available to all Member States) where a Member State that intends to issue a European Investigation Order fills in a form indicating the target country, which is immediately translated into the language of the target country. This will put an end to the paper-based procedure and will even ban the sending of the European Investigation Order.

I believe that through the literature and the spontaneous interviews conducted, we have gained an insight into current situations in practice, and through them, we have been able to see the impact of Covid-19 on international cooperation instruments in criminal matters, as well as plans for the near future. One thing is certain: the multifaceted support of international organisations is essential for both police and judicial cooperation.

Finally, I will conclude my paper with the thoughts of Deputy Commissioner General Henrik Dorning, who formulated the foundations of international cooperation in criminal matters almost 100 years ago. "International cooperation is important for the police of every country. Here are the roots of common threads running from all sides and this has made necessary and possible the need to build the basis for international relations."[36]

References

Act LIV of 2002 on the International Cooperation of Law Enforcement Agencies.

Act CLXXX of 2012 on Cooperation with the Member States of the European Union in Criminal Matters.

Csákó, Beáta (2016): Bűnügyi együttműködés az Európai Unióban. *Információs jegyzet, Országgyűlés Hivatala*, 2016/37.

Dornfeld, László (2020): A koronavírus-járvány hatása a kiberbűnözésre. *In Medias Res*, 9(4), 193–204.

Dorning, Henrik (1937): *A bűnügyi rendőrség nemzetközi összeműködése.* Budapest: Pallas.

Dorning, Henrik (1942): A bűnözés nemzetközi hálózata. In Borbély, Zoltán – Kapy, Rezső (eds.): *A 60 éves magyar rendőrség 1881–1941*. Budapest: Halász Irodalmi és Könyvkiadó Vállalat. 167–170.

Eurojust (s. a.): *What We Do.* Online: www.eurojust.europa.eu/about-us/what-we-do

European Commission (2021a): *Melléklet a következőhöz, Javaslat A Tanács határozata a tagállamoknak a számítástechnikai bűnözésről szóló egyezményhez csatolt, a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról szóló második kiegészítő jegyzőkönyvnek az Európai Unió érdekében történő megerősítésére való felhatalmazásáról.* Brussels: 25 November 2021.

European Commission (2021b): *Joint Investigation Teams (JITs) Collaboration Platform.* Online: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/digitalisation-justice/joint-investigation-teams-jits-collaboration-platform_en

European Commission (s. a.): *A határok nélküli Európa. A schengeni térség.* Online: https://doi.org/10.2837/47559

European Council (2019): *Zárójelentés a kölcsönös értékelések hetedik fordulójáról, A számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet érintő európai szakpolitikák gyakorlati végrehajtása és működése.* Brussels: 15 November 2019.

European Council (s. a.): *The EU's Fight against Organised Crime.* Online: www.consilium.europa.eu/en/policies/eu-fight-against-crime/

European Judicial Network (s. a.): *Hungary, Judicial Cooperation.* Online: www.ejn-crimjust.europa.eu/ejn2021/ContentDetail/EN/5/13

European Union Agency for Criminal Justice Cooperation (s. a). Online: www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network

[36] Dorning 1942: 167–170.

Europol (2020): *How Covid-19-related crime infected Europe during 2020.* Online: www.europol.europa.eu/cms/sites/default/files/documents/how_covid-19-related_crime_infected_europe_during_2020.pdf

Hegyaljai, Mátyás (2014): Az EMPACT mint rendészeti válasz az európai bűnözésre. In Gál, Gyula – Hautzinger, Zoltán (eds.): *Tanulmányok a „biztonsági kockázatok – rendészeti válaszok" című tudományos konferenciáról.* Pécsi Határőr Tudományos Közlemények, 15, 127–134.

Kolozsi, Bálint (2022): Nemzetközi bűnügyi együttműködés, közös nyomozócsoport magyar–német–román relációban. *Belügyi Szemle,* (70)2, 277–303. Online: https://doi.org/10.38146/BSZ.2022.2.4

Közbiztonság, 22 August 1869. 1.

Közbiztonság, 23 April 1911. no. 17. 222.

Monroy, Matthias (2020): *Security Architectures in the EU. EU Police Forces Plan New Information System.* Online: https://digit.site36.net/2020/09/16/eu-police-forces-plan-new-information-system/

Nagy, Ivett (2021): A kábítószer-bűnözés átalakulása az online platformok hatására [Drug Crime Transformation under the Effect of Online Platforms]. *Belügyi Szemle,* 69(6), 107–123. Online: https://doi.org/10.38146/BSZ.SPEC.2021.6.7

Nagy, Zoltán (2021): *A karantén krimogén veszélyei.* Online: https://ujbtk.hu/dr-nagy-zoltan-a-karanten-krimogen-veszelyei/

Nyeste, Péter (2020): A nemzetközi bűnügyi együttműködés és a leplezett eszközök. Ruzsonyi, Péter (ed.): *Közbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok III.* Budapest: Ludovika Egyetemi Kiadó. 833–852.

Páhi, Barbara (2019): A nemzetközi bűnügyi együttműködés, különös tekintettel az Európai Közösség pénzügyi érdekeinek védelmére. *Miskolci Jogtudó,* (1), 57–68.

Sallai, János (2015): A rendészet kihívásai napjainkban. *Hadtudomány,* 25(1–2), 135–138. Online: https://doi.org/10.17047/HADTUD.2015.25.1-2.135

Sallai, János – Borszéki, Judit (2022): A nemzetközi rendőri együttműködés kezdetei. *Belügyi Szemle,* 70(5), 983–1003. Online: https://doi.org/10.38146/BSZ.2022.5.6

Szijártó, István (2019): Az Europol és az Eurojust szerepe a közös nyomozócsoportokban. *Ügyészek Lapja,* (6).

Southeast European Law Enforcement Center (s. a.). Online: www.selec.org/

Szomora, Zsolt (2022): *A 20 éves Budapesti Egyezmény II. Kiegészítő Jegyzőkönyvét 2022 májusában nyitja meg aláírásra az Európa Tanács* [The Second Additional Protocol to the 20th Anniversary Budapest Convention Will Be Opened for Signature by the Council of Europe in May 2022]. Online: https://jogaszegylet.hu/jogelet/a-20-eves-budapesti-egyezmeny-ii-kiegeszito-jegyzokonyvet-2022-majusaban-nyitja-meg-alairasra-az-europa-tanacs/

AARMS Vol. 22, No. 1 (2023) 51–60.

10.32565/aarms.2023.1.4

The Role of Locality in Public Service Management of Ecuador

A Sense of Competitive Cities[1]

Stefany CEVALLOS[2]

The Ecuadorian Government with the aim of planning and making decisions in real time should include the perspective of a new city model in function of the new social needs and the construction of an image for its own country and the international arena. Foreign Direct Investment (FDI) should be a fundamental support for these to provide jobs for youths and the ability to generate new businesses. Nowadays, there are public decision-making processes to influence public policy. The author seeks to reflect on local governments and their current perspective regarding the provision of services. Indeed, public management plays a fundamental role in the development of different programs in the field of the digitalisation of services to generate viable solutions and try to improve the quality of life of its inhabitants. Methodology: secondary sources were used for content analysis based on the overview of relevant literature written in English and Spanish.

Keywords: *locality, decentralisation, public administration, governance, Ecuador*

Introduction

While it is true that there is no model of good governance, it is also necessary to emphasise the measurement of results for ideological reasons. Governance is ultimately the way of regularising the interactions between the actors in society that can be democratic or authoritarian. The analysis of the public policies takes the set of plans as an object of study shaped for: the collective aims that the State considers to be desirable or necessary (including the process of definition and formation of these), the means and actions used, total or partially, for an institution or governmental organisation, and the results of these actions, including so much the consequences wished as the unforeseen ones.[3]

---

[1] The present publication was presented in an oral form on the *II South America, South Europe International Conference* at the Ludovika – University of Public Service, Budapest, Hungary, on 3–5 March 2022.

[2] PhD student, University of Public Service, e-mail: stefy220_@hotmail.com

[3] Roth Deubel 2007.

Promoting good governance goes beyond the local government and includes the private sector and society. There are two moments: the rule of law, so much as the Constitutional state from which it emanates is subject to the rights of individuals; and the second being the recognition of several normative systems different from the law produced by the national assembly, consequently multiplying the sources of law. In this case, Public–Private Partnerships is in force in Ecuador since late 2015.[4]

The political organisation of Ecuador is a republican regime. In Ecuador the participatory democratic system is the foundation of its political authority. The Organic Code on Territorial Organization and Decentralization (COOTAD) is the maximum norm of the Decentralized Autonomous Governments (GAD) in Ecuador and determines that local government is ruled by the principles of unity, solidarity, co-responsibility, subsidiarity, complementarity, interterritorial equity, citizen participation and sustainability of development. During the administrative management, the elected local authority must provide for both the fulfillment of the action plan of its electoral campaign, as well as the Territorial Development and Planning Plan (PDOT) in the main planning instruments, which contribute to the monitoring of compliance with the objectives of public management. A management period begins with the inaugural session of the new authority. It is propitious momentous to carry out a governability pact from public institutions and a governance pact that includes the participation of citizens in local development. To deepen knowledge about political legitimacy and good governance in the local governments, this report includes a case single-country study about the general effect of both political governance and legitimacy in international treaties as predictors of support governance in Ecuador. In all aspects of public and private life, "branding" is a significant effort that signifies spending money on urban marketing strategies to be crucial in regional management and development. Global statistics clearly show that countries spend money in public funds on branding strategies to attract FDI.

In this context, the governance system at the external level is fostering a culture of transparency based on criteria of co-responsibility, institutional strengthening and participation. However, this article considers necessary and fundamental to hold a wide-ranging debate on this question, assessing the positive and negative aspects of the possible adoption of new management systems.

Decentralisation

In the Socialism of the 21st century context, decentralisation in Latin America could be seen as an alternative to deal with the inefficiency of local governments. Indeed, it is a political speech that highlights the desire to eliminate the concentration of power in large cities and thus a lack of services to citizens in locations where inhabitants are abandoned. On this subject, the Ecuadorian author Fernando Carrión M.[5] states that the reader should

[4] In Ecuador, Decree Nº 582 on Public–Private Partnership (Asociación Público Privada) of 2015 is the most important document for future investors.

[5] Carrión 2007: 36–52.

not be confused and must be experienced with the concept of decentralisation as a holistic process to prevent further centralisation.[6]

Services to citizens

Local governments in Ecuador work under the Organic Code of Territorial Organization, Autonomy and Decentralization (COOTAD) and as such the tasks are the provision of services to their constituents. When talking about locality, proximity to the population is a very important consideration to meet the concrete needs. Certainly, prioritising the problems is also an important issue and the seriousness of the impact and damage they involve.[7]

COOTAD establishes the political-administrative organisation of the Ecuadorian State in the territory, the regime of different levels of decentralised autonomous governments and special regimes to guarantee their political, administrative and financial autonomy. The Decentralized Autonomous Governments are the institutions that make up the territorial organisation of the Ecuadorian State and are regulated by the Constitution of the Republic of Ecuador (Articles 238–241). In addition, it develops a mandatory and progressive decentralisation model through the national system of competencies. The institution is responsible for its administration, sources of financing, and the definition of policies and mechanisms to compensate for imbalances in territorial development.

In this context, the decentralised government consists of decentralised institutions that have political, administrative and financial autonomy, and are governed by the principles of solidarity, subsidiarity, equity, interterritorial integration and citizen participation. They are organised as follows: Regional; Provincial; Cantonal and Parish. Within the functions attributed to it by Article 119 of the Organic Code, it "coordinates processes of institutional strengthening and technical support for the exercise of powers to decentralised autonomous governments" and "promotes and monitors compliance with citizen participation mechanisms in the management of decentralised autonomous governments".

Before going into detail, the following services should be seen as priorities for certain authorities but not others. The services are the following:

- Drinking water, drainage, sewage, treatment and disposal of wastewater
- Public lighting
- Cleaning, collection, transfer, treatment and final disposal of waste
- Markets and supply centres
- Cemeteries
- Flea markets
- Streets, parks and gardens and their equipment
- Public security

---

6 Carrión 2002.

7 Moon–Kendall 1993.

Once every four-calendar year, priorities attention are pre-defined and reflected by the new Government Plan presented by the political candidate at the time, and once he or she comes to power, he or she shall put it into practice with the institutional oversight already the case.

These participation formulas where citizens are increasingly having a minimum quantifiable number of participations is a relevant dilemma and it is an issue of access to fundamental services such as health, water, public education, transportation, air management, and technological gap covered by the private sector. Indeed, inorganic growths, social segregation, environmental commitments of water and air, violence and citizen insecurity, institutional difficulties and social gaps are remaining the same.[8]

The dominant conceptions

Dynamics of decentralisation in local governments[9] is not a strictly technical process; it is rather a field of conflicting and diverse interests that are embodied by specific actors e.g. private actors, public sphere, civil society and different actors. Undeniably, conflict of interest within the political institutions is real and we cannot shrink from our responsibility to combat it, although the political discourse claims the exact opposite in the same speech.

A sense of competitive cities

There is a process of transformation in the society–state relationship, which is expressed in the approximation of civil society to the municipality through new forms of participation and representation of the population and the granting of more power to the autonomous bodies. Eminently urban service is capable of promoting due to their omnipresent nature in the process of contact with inhabitants' new social subjects such as young people, athletes, women, environmentalists, etc.

So, if the current decentralisation proposal seems to perform adequately, what makes it new today and what are its characteristics and elements of power? The answer could be that sense of competitive cities that comes hand in hand with a hegemonic model imposed by a double trilogy: opening (globalisation), economic restructuring (adjustment) and state reform (privatisation), inscribed within the globalisation/locality dilemma.

Having mentioned some points in detail that give rise to locality around the public service, power, culture and economy. The problem of decentralisation is part of the contradictory movement that our society is experiencing, which is expressed in the processes of globalisation and seen increasing the importance assumed by the local government.

The first conception starts from a critique of the state, from a perspective of participation of the "civil society" through the so-called processes of privatisation, market expansion

[8] Bonbright et al. 1988.
[9] Barrera Guarderas 2007.

and maximisation of consumer sovereignty. That shared discourse that comes from the premise that the public sector is usually ineffective. Furthermore, it is a mechanism for diffusion and generalisation of the market, which breaks up demand and atomises conflicts.

The second conception seeks the democratisation of the State, rationalising public administration (emphasising the territorial rather than the sectoral), promoting governance at all levels, sponsoring economic development, generating better national integration (not homogenisation) and expanding the population participation. The most significant case is the Ecuadorian Constitution, which starts with the constitution approved in 2008.

Competition vs. competitiveness

There is a trend towards increasing powers at the local level, either due to the increase in local demands or due to the transfer of central bodies.

This growth of competences does not make sense if the corresponding body does not have the capacity to assume them;[10] much more in countries as Brazil and Ecuador where the municipalities can do what they see fit, without being obliged to do anything.

Hence, the problem now is, more than the transfer of competences, the corresponding increase in resources because, otherwise, a "perverse" logic would be entered.[11]

The governance system determines legal instruments of accountability, of decision-making. In this respect, the instruments of urban marketing are going to evolve because of the incidences of non-State actors. Social organisations as actors in the dynamics of governance are multiplying according to the communities and can act in union activities or political activities. These include civil society organisations in governance policies under the umbrella of governance. Besides, States have implemented changes to national legislation towards economic development. A manner of achieving legal and policy changes to protect and advance foreign investment.

Public–Private Partnership

Public–Private Partnership or Asociación Público Privada is experiencing growth in almost all the South American region.[12] In 2015, Decree Nº 582 on Public–Private Partnership (Asociación Público Privada) became the most important document for future investors. As a form of privatisation derived from the USA, it was successfully applied in European Union countries,[13] but many authors realised at the same time that it can easily become the hotbed of corruption, so they elaborated sample contracts to it and recommended them to the EU member states to apply.[14]

---

10 Ashworth–Page 2011: 1–15.
11 Ashworth–Kavaratzis 2007: 520–531.
12 Reyes-Tagle et al. 2021.
13 Lacasse–Wall 1994.
14 Rosenbloom 1986.

In Ecuador, in the context of post-Socialism of the 21st century, the current government is re-launching neoliberal paradigms that in fact are the introduction of business methods considered possible by the New Public Management. The technique of the performance of public tasks[15] is "contracting out", i.e. "public–private partnership" (PPP).[16]

New Public Management considers the implementation of economic and other public goals to be the most successful using management techniques. These include the decentralisation of decision-making mechanisms, planning, analysis, feedback and the application of new management principles. These management techniques have always been widely used by businesses and are considered by many to be applicable to the operation of public administrations.

Setting limits

Resistance to change, insofar as it is presented as a cultural and administrative obstacle for people, social actors and institutions that are breaking with inertial processes in which they are immersed.[17] In fact, centralism, as a social relationship that has its local and national support bases, opposes to decentralisation to the extent that its main actors lose the privileges it gives them. So, central government justifies its attitude by the low capacity of local entities to assume the new significate rages of powers. Inter alia, the scattering of resources does not allow development, and the difficulty of controlling corruption.

A social and urban analysis approach from governance

There is a problem of provision, administration and management of public services. For example, social disintegration is a scenario where neighbourhoods with high coverage versus marginal influence itself on the international and national political systems that establish levels of governance. International organisations spread preponderant normative criteria of good governance from a neoliberal approach to regulationist governance that have become a central concept used by designer politicians and authorities at the local, national, regional and global level, and by social sciences, too.[18]

In this respect, the instruments of the decentralisation process are going to evolve as a result of the incidence of non-State actors or private institutions. Social organisations as actors in the dynamics of governance are multiplying according to the communities, and can act in union activities or political activities. These include civil society organisations in governance policies.

---

15 Banco Interamericano de Desarrollo s. a.
16 Mulreany–Devlin 1998.
17 Ashworth–Voogd 1990.
18 Waylen 2008: 114–135.

However, the emergence of the Constitutional State occurred with the rupture of the sense of sovereignty, in which the State ceased from being politically "everything" to simply becoming a "part" of more comprehensive political systems (the rule of law).

Although its political reality could no longer be recognised as a functioning political reality, since the late twentieth century, there have been vigorous internal and external corrosive forces that weakened the sense of sovereignty of the rule of law such as: the internal political and social pluralism, which opposes to the idea of sovereignty and subordination, the formation of an alternative and competing power with the State.

Furthermore, operating in the political, economic, cultural and religious fields, the progressive institutionalisation, promoted sometimes by the States themselves, of "contexts" that integrate its power and the supranational dimensions, removing them this way to the availability of the particular States, and the attribution of rights to individuals, who can assert them before international jurisdictions against States to which they belong.[19]

An additional element inside the configuration of the State that Zagrebelsky raises is the concept of the Constitutional state as a uni-directional value of the State development organisation. The typical form of the State in our century is presented often as a particular version of the Constitutional state where the general sense of the liberal State of law consists of the conditioning of the authority of the State to the freedom of society, within the framework of the reciprocal balance established by the law.

Nevertheless, the Constitutional law makes way to the Constitution and becomes itself the object of measurement. The outlook of the State towards a democratic pluralist and participative construction of social group is given depending on the "analysis of the public policies" orientated to perceiving the State with few consecration or reverence.[20] This analysis does not imply trying to reduce the State to a common and current organisation; nevertheless, it thinks that the State and its institutions shall be analysed like "organizations across which the public agents (chosen or administrative officers) chase goals that do not exclusively answer social demands and, simultaneously, as configurations of organizations and actions that they structure, shape and influence both the economic processes and the classes or groups of interest".[21]

The analysis of the public policies takes the set of devices as an object of study shaped for: the collective aims that the State considers being desirable or necessary (including the process of definition and formation of these),[22] the means and actions used, total or partially, for an institution or governmental organisation, and the results of these actions, including so much the consequences wished as the unforeseen ones.[23] Furthermore, Ecuador has stable and successful policies that offer confidence and benefits to foreign investors to attract FDI. Investment Promotion Agencies are the institutions responsible for promoting foreign investment in a specific area. These types of institutions may be governmental, non-profit organisations and even private entities run by boards of directors, which may include government officials and business managers. Therefore, one of the main activities

19 Zagrebelsky 1995.
20 Castells 1968: 72–90.
21 Roth Deubel 2007: 18.
22 Cabrera-Jara 2019a.
23 Roth Deubel 2007: 21.

of an Investment Promotion Agency is the positioning of the country in the international market, a task that implies the construction of a favourable image, and with this, the creation of a "Country Brand".

Conclusions

The author concludes with some final considerations: Decentralisation is a claim and a viable possibility in today's Latin America because society has become urbanised, there is great accessibility to the media, illiteracy levels have been reduced, civil society has important and diverse forms of organisation, and the tradition of local governments has been cemented in recent years. This demonstrates that the social actors of decentralisation can enter into a transition process as agents of diffusion of development, as instances of expansion of representation and as ambits of the constitution of multiple identities. Decentralisation is a condition for the modernisation of the Latin American State and society, insofar as it deepens democracy, improves governance and fosters economic development. In other words, the discussion of the modernisation of the State requires incorporating the criteria of territorial democracy and decentralisation, in order to allow a real reform of the articulation of the State and civil society. This supposes some of the following additional reflections: Decentralisation is a long process and not an episodic event – such as the approval of a Law – that has multiple components that are defined in time and space.[24] Decentralisation is a holistic process that does not solve everything, but it has to do with everything: democracy, development and governance. Restricting it to a single scope can lead to situations of greater centralisation.

Concerning to PPPs, there is a limitation for local governments when transferring the execution of public service to private administration. Weaken the public system and validate the concept that the public system is obsolete and in effect neglects the subsidy of social services in a country where social gaps are latent and, poverty constitutes a high index that has worsened by the global crisis due to the Covid-19 pandemic, Putin war and the crisis of organized crimes. In spite of the national scene, achieving the Development Goals is the responsibility of the governments and local governments, the same one that allowed the countries to place in the international agenda the need to work on areas where a major degree of poverty was demonstrated and to give priority and treatment to the construction of a new image for international investors.

References

Ashworth, Gregory – Kavaratzis, Mihalis (2007): Beyond the Logo: Brand Management for Cities. *Journal of Brand Management,* 16(8), 520–531. Online: https://doi.org/10.1057/palgrave.bm.2550133

[24] Carnap 1950.

Ashworth, Gregory – Page, Stephen J. (2011): Urban Tourism Research: Recent Progress and Current Paradoxes. *Tourism Management*, 32(1), 1–15. Online: https://doi.org/10.1016/j.tourman.2010.02.002

Ashworth, Gregory J. – Voogd, Hendrik (1990): *Selling the City. Marketing Approaches in Public Sector Urban Planning.* London: Belhaven Press.

Banco Interamericano de Desarrollo (s. a.): *APP en la Región Servicios de Asesoría.* Online: https://bit.ly/2xJHZAY

Barrera Guarderas, Augusto (2007): Agotamiento de la descentralización y oportunidades de cambio en el Ecuador. In Carrión, Fernando M. (ed.): *La descentralización en el Ecuador: opciones comparadas.* Quito: FLACSO/SENPLADES. 175–206.

Bonbright, James C. – Danielsen, Albert L. – Kamerschen, David R. (1988): *Principles of Public Utility Rates.* Arlington, Virginia: Public Utilities Reports Inc.

Carrión, M. Fernando (2007): El desafío político de gobernar la ciudad. *Nueva Sociedad*, (212), 36–52.

Carrión, M. Fernando (2002): La descentralización en América Latina: una perspectiva comparada. In *Procesos de descentralización en la comunidad Andina.* Quito: FLACSO-OEA.

Cabrera-Jara, Natasha (2019a): Gentrificación en áreas patrimoniales latinoamericanas: cuestionamiento ético desde el caso de Cuenca, Ecuador [Gentrification in Latin American Heritage Areas: Ethical Questioning Based on the Case of Cuenca, Ecuador]. *urbe. Revista Brasileira de Gestão Urbana*, 11. Online: https://doi.org/10.1590/2175-3369.011.e20180201

Cabrera-Jara, Natasha (2019b): Mercado inmobiliario y metamorfosis urbana en ciudades intermedias. Gringolandia en Cuenca: la tierra prometida [Real Estate Market and Urban Metamorphosis in Intermediary Cities. Gringolandia in Cuenca: The Promised Land]. *Bitácora Urbano Territorial*, 29(1): 91–100. Online: https://doi.org/10.15446/bitacora.v29n1.75223

Carnap, Rudolf (1950): *Logical Foundations of Probability.* Chicago: University of Chicago Press.

Castells, Manuel (1968): Y a-t-il une sociologie urbaine? *Sociologie du travail*, 10(1): 72–90. Online: https://doi.org/10.3406/sotra.1968.1380

EC Asamblea Nacional: *Constitución de la República del Ecuador 2018.* Online: https://bit.ly/3eLSowO

EC Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD). Online: https://bit.ly/3czprCh

EC Consejo Nacional Electoral "Transparencia 2017" CNE. Online: https://bit.ly/2Vot7Rr

EC Dp World. "Desarrollo Local Posorja". Online: https://bit.ly/2VIYzcb

EC Gobierno Autónomo Descentralizado Provincial de Santo Domingo de los Tsáchilas (GADPSDT) (2020): *APP Puerto Seco Santo Domingo.* Online: https://bit.ly/34R4EaA

EC Ley Orgánica de Incentivos para Asociaciones Público-Privadas y la Inversión Extranjera. Online: https://bit.ly/2xGj29J

EC Ley Orgánica para el fomento productivo, atracción de inversiones, generación de empleo, y estabilidad y equilibrio fiscal. Online: https://bit.ly/2TlrAdA

Fontaine, Guillaume (2010): *Petropolítica. Una teoría de la gobernanza energética.* Quito: FLACSO. Online: https://doi.org/10.14201/alh.7793

González, Matías – Boza, José – De León, Javier (2018): Buen gobierno y eficacia de la ayuda al desarrollo. *Criterio Libre,* 16(29), 143–162. Online: https://doi.org/10.18041/1900-0642/criteriolibre.2018v16n29.5012

Green, Amelia – Grace, Debra – Perkins, Helen (2016): City Branding Research and Practice: An Integrative Review. *The Journal of Brand Management,* 23(3), 252–272. Online: https://doi.org/10.1057/bm.2016.8

Hospers, Gert-Jan (2010): Lynch's *The Image of the City* after 50 Years: City Marketing Lessons from an Urban Planning Classic. *European Planning Studies,* 18(12), 2073–2081. Online: https://doi.org/10.1080/09654313.2010.525369

Lacasse, François – Wall, Terry (1994): *Public–Private Partnerships in Infrastructure Provision: Main Issues and Conclusions.* Paris: OECD, Public Management Occasional Papers, 1994/6.

Lynch, Kevin (1960): *The Image of the City.* Cambridge, Mass.: The MIT Press.

Moon, Graham – Kendall, Ian (1993): The National Health Service. In Farnham, David – Horton, Sylvia (eds.): *Managing the New Public Services.* London: Palgrave. 172–187. Online: https://doi.org/10.1007/978-1-349-22646-7_8

Mulreany, Michael – Devlin, Liam St John (1998): *Public Expenditure and the Private Sector.* London: Institute of Public Administration.

Objetivos de Desarrollo Sostenible (ODS) 2030. Online: https://bit.ly/3boZyF7

Programa de Naciones Unidas para el Desarrollo Agenda 2030 "Ranking Business in Latin America and Caribbean". Online: https://bit.ly/3boZyF7

Reyes-Tagle, Gerardo – Ponce de León, Oscar – Brandão, Luiz Eduardo T. – Celle, Adilio – Dompieri, Izabel – Grijalva, Jose – Martins Vieira, Cynthia – Rebollo, Andres – Ventim, Bruno (2021): *Impacto fiscal en APP en América Latina y el Caribe.* Banco Interamericano de Desarrollo. Online: https://doi.org/10.18235/0003780

Rosenbloom, David H. (1986): *Public Administration. Understanding Management, Politics and Law in the Public Sector.* New York: Random House.

Roth Deubel, André-Noël (2007): *Políticas públicas. Formulación, implementación y evaluación* [Public Policies: Formulation, Implementation and Evaluation]. Bogota: Aurora.

UNCTAD (2019): Promoting Investment for Sustainable Development in Cities. *The IPA Observer,* (7), 1–9. Online: https://bit.ly/2RUL2x3

Waylen, Georgina (2008): Gendering Governance. In Goertz, Gary – Mazur, Amy G. (eds.): *Politics, Gender, and Concepts. Theory and Methodology.* Cambridge: Cambridge University Press. 114–135. Online: https://doi.org/10.1017/CBO9780511755910.006

World Bank (s. a.): *APP in Latin America and Caribbean.* Online: https://bit.ly/2zgEi6g

Xiaohu, Zhang – Menglong, Li (2019): Meta-governance as a New Solution to the Governance Crisis. *Management Issues,* 39(3), 88–93. Online: https://doi.org/10.22394/2304-3369-2019-3-88-93

Zagrebelsky, Gustavo (1995): *El derecho dúctil. Ley, derechos y justicia.* Madrid: Trotta.

AARMS Vol. 22, No. 1 (2023) 61–75.

10.32565/aarms.2023.1.5

Historical Forms of Just War Theory in Europe and Hungary[1]

Mihály BODA[2]

Just war thinking features the history of warfare from the beginning up to the 20th century. Just war thinking, however, did not have one unique frame, but it appeared in many forms. The theory of judgement of God, the mission-related theory, the law enforcement theory, the revolutionary, and finally, the regular war theory were the important forms of historical just war thinking. This article presents these theories and classifies them with the help of the main concepts of Saint Thomas Aquinas and the principal concepts of justice.

Keywords: *just war theory, revolutionary war, regular war theory, judgement of God, idea of the Holy Crown*

Introduction: Theory, tradition and just war thinking

If someone is thinking about warfare justice nowadays, just war theory can easily come into mind. Although just war theory induces debates on some points, it is relatively a well-elaborated and well-recognised system of rules of war. These rules can earn some role in practice before the decision of going to war as a justificatory device, just like after the war as its evaluation.[3] Besides just war theory, one can refer to just war tradition as well. According to the tradition-related approach, rules of justice have a central role in the morality of war, but they do not constitute a commonly accepted and practically applicable device.[4] These two approaches can be combined by saying that elements of the theory should be built on the tradition.[5] This combination of tradition and theory emphasises the uniformity of traditional warfare justice. Finally, we can discern some or perhaps many forms of just war thinking in the tradition of just war. This concept accentuates the complex nature of warfare justice, and so the different forms of warfare justice. In this article I present some European and Hungarian forms of just war thinking from the early Middle Ages to the 20th century. I apply the essential categories of the just war theory of

1 This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.
2 Associate Professor, Head of Department, University of Public Service, Department of Military History, Philosophy and Cultural History, e-mail: boda.mihaly@uni-nke.hu
3 McMahan–McKim 1993: 501–541; Frowe 2011: 50–69.
4 Johnson 2006: 167–195.
5 Walzer 1992: 44–45.

Saint Thomas Aquinas and some related concepts of justice as a proper framework to distinguish the different forms of just war thinking.

The framework: Saint Thomas Aquinas's essential categories of just war

Saint Thomas Aquinas (1225–1274) in his *Summa Theologiae II–II* gives the answer to the question of 'Whether any war is licit?' that in order for a war to be licit (just) three conditions are required. These are in general:

- *acturitas* (legitimate authority): there should be a person entitled to start the war
- *causa iusta* (just cause): there should be an immediate just cause of starting the war
- *recta intentio* (right intention): the war should be intended as the advancement of good, that is there should be a further goal of starting the war[6]

One can hold these conditions being equally important in warfare justice, others can prefer legitimate authority to just cause and right intention, or just cause to right intention and legitimate authority, or right intention to legitimate authority and just cause. Taking the latter option, we can discern three basic forms of just war thinking: the first one builds on the legitimate authority condition, the second one stresses the just cause condition, and the third one takes the right intention condition as a basis.

Saint Thomas's theory is a form of just war theory, for this reason his main conditions are connected to the different forms of justice. Justice, taking it on the highest abstract level, is giving everybody what is their due.[7] Justice has several forms, like procedural, redemptive, corrective (rectificatory), distributive and legal justice. Procedural justice rose into view in social sciences in the seventies. Then it was connected to distributive justice and was applied to evaluate the outline of social exchange and facilitated the justice of it. In this case we should take first the definition of distributive justice, and then take the just procedure which can reach just distribution.[8] However, much earlier in the history of thinking a different form had been appeared. According to the medieval jurist Gratian (11–12th century) a "judge is called such because he pronounces justice (*ius dictat*) to the people, or because he adjudicates (*disceptet*) justly. To adjudicate justly is to judge justly. For he is no judge who has no justice within himself".[9] In this definition justice is observed after the adjudicating procedure and is secured by the procedure only without any prior definition. Redemptive justice "is with special bias in favor of the helpless who can contribute nothing at all and are in fact 'due' nothing" according to the Christian thinker Paul Ramsey (1913–1988).[10] In contrast to procedural justice, helplessness appears before the process of taking care of the helpless is terminated and defines the main feature of this form of justice. Helplessness is a negative characteristic, it means something is

6 Aquinas 2013b: 177.
7 Mille 2021: 1.
8 Rawls 1999: 74; Bobocel–Gosse 2015: 51–88.
9 Gratian 2013: 113.
10 Ramsey 1978: 14.

missing, and it is not a due only in this sense. Helping the needy is, however, a form of duty, and not only an act of praiseworthy charity, and for this reason it is a form of justice. Corrective (rectificatory) justice, according to Aristotle (384–322 B.C.): "The other kind of justice is rectificatory, which is found in both voluntary and involuntary transactions. […] What is just in transactions is nevertheless a kind of equality […]. The law looks only to the difference made by the injury, and treats the parties as equals, if one is committing injustice, and the other suffering it – that is, if one has harmed, and the other been harmed. So, the judge, since this kind of injustice is an inequality, tries to equalize it".[11] Corrective justice can already be observed before the judge makes his decision (it in fact grounds the decision of the judge), because it is connected to a previous injustice and the connected due on the side of the aggrieved party and the offender party as well. It is just to compensate the aggrieved party for his loss and punish the offender party for his deed. Distributive justice, according to Aristotle, is "always in accordance with the proportion stated above, since if the distribution is from common funds, it will be in the same ratio as are the corresponding investments to one another. And the injustice that is opposed to this kind of justice is what violates the proportion".[12] Unjust distribution and social exchange of the goods bring about due on the side of the harmed party, and on the profiteer party as well. Finally, legal justice is linked to political life. According to Aristotle what is "legal is what originally makes no difference whether it takes one form or another, but does matter when people have adopted it; for example, that the ransom for a prisoner be one mina…".[13] The content of legal justice depends on the will of special actors like the representatives of the national legislative body or the members of the international community. After the acceptance of the content as legally compelling content of an act, it is equally available and binding to every member of the national or international community. So, if one or the other member violates it, it commits legal injustice.

These main forms of justice match the required conditions of Saint Thomas Aquinas: procedural justice to legitimate authority condition, redemptive justice to right intention condition, and the remaining forms to the just cause condition. Hence, these forms of justice suit well to the different forms of just war thinking. In the following I distinguish five forms of just war thinking with the help of the conditions of Saint Thomas Aquinas and the shown forms of justice.

Historical forms of just war thinking

There are three basic forms of just war thinking. They are built on the concept of legitimate authority, or the concept of just cause, or the concept of right intention and the related ideas of justice. In this section I am presenting these basic forms starting with the legitimate authority-related just war thinking, following with the right intention-related theory, and finally coming to the more complex just cause-related theories.

[11] Aristotle 2004: 1132a. 87.
[12] Aristotle 2004: 1131b. 87.
[13] Aristotle 2004: 1134b. 93.

Legitimate authority: Just war as judgement of God

According to just war thinking based on legitimate authority just wars are those victorious wars which have been won by the just judgement of God.[14] In details:

- justice of war is a consequence of God's judgement which is the result of the functioning of God's just judging ability, and so it is procedural justice
- the necessary consequence of God's judgement that a war is just is the victory in war showing *ex post facto* which was (is) the just party in the war (the defeated side was (is) the unjust party)
- God's judgement can be influenced by just and pious peacetime and wartime behaviour of the king and his people, however
- God starts or organises the war Himself

An important example of just war thinking based on legitimate authority is the political theology and the connecting warfare theory of Isidore of Seville (560–636). According to Isidore, Christ is the perpetual king and priest at the same time, and the Church, the baptised people are His body. This unified godly empire can be followed by a politically divided earthly Christian empire, like the different Christian–German kingdoms contained by the Western Christian world in the early Middle Ages. These kingdoms are the cells of the Church and are ruled by earthly (human) kings. A kingdom is a present of God to the king, who is at the same time vested responsibility for taking care about his subjects. Kings should set good example in practicing the virtues of justice and piety to their subjects. Kings have to be just regarding the Christian ideals and the local customs as well, so kings are Christian priests and members of the local German community. Kings should be pious at the same time to their people which is restriction of excessive strictness of just judgements. In exchange, the subjects' God given obligation is to obey to the kings. Kings are also supposed to maintain Christian and customary laws and to extend the just and pious form of life by applying violence if it is necessary. Wars are important means of founding and extending Christian kingdoms.[15]

Beyond his political theology, Isidore mentions and defines just war particularly. His definition comes from Cicero: "Those wars are unjust that are taken up without due cause, for except for the cause of avenging or of driving off the enemy no just war can be waged."[16] This definition shows Isidore's awareness and acceptance of the Roman approach only. However, in the 12th century Gratian used this definition with an additional part, which he supposedly ascribed to Isidore: "A judge is called such because he pronounces justice (*ius dictat*) to the people, or because he adjudicates (*disceptet*) justly. To adjudicate justly is to judge justly. For he is no judge who has no justice within himself."[17] This supplement, which is related to the concept of just war in Gratian, deduces justness of a judgement from the justice of the judge. Further, this supplement can also be found in Isidore's text, some

[14] Boda 2021a: 63–67; Boda 2022b.
[15] Isidore of Seville 2006: 117–118, 199–200, 359–360.
[16] Isidore of Seville 2006: 359.
[17] Gratian 2013: 113.

pages after the Ciceronian definition of just war.[18] The combination of the two parts, with the political theology in the background, shows that Isidore holds the judgement of God theory in which procedural justice has eminent role.

This form of just war thinking lies on God's judgement which justifies the deeds and lifestyle of the king and his people backward in time.[19] God judges the just and unjust deeds always in the present and connects His judgement necessarily to the realisation of that judgement, to victory or punishment.[20] According to Isidore, the attack of Attila and the Huns was God's punishing judgement and its realisation.[21]

God's judgement is not entirely unpredictable for people, so they are able to influence that by just and pious, or even unjust and impious lifestyle. However, influence is not equal with determination, so one cannot be certain that their influence will be successful, because God's judgement concerns all the connecting deeds of the past, present and future as well,[22] most of which are knowable only for Him. Even the most pious men cannot have hundred percent certainty in principle (however, according to Isidore, the just men understand that they are only tested in adversities).[23] If the king and his people live on the standards of God then God "lives in them"[24] and hence starts their war. This is possible because all the earthly things were formed as being in God, and man particularly was created in the image of God.[25] However, if the king and his people disrespect God's rules then God starts a war against them by organising other peoples (like the Huns) for attacking them as the "scourge of God's fury".[26] So God starts the war of the king and his people, judges that war, and makes it victorious or lost. God, however, makes the decision on the just or unjust nature of a particular war by starting that war, His judgement becomes clear for the men by the victory or defeat at the end of war.

Right intention: Just war as mission

Just war thinking based on right intention takes mission-related wars as just wars, which have the following character: it violently purposes to build or maintain a political rule in order to take care in some way of the needs of the (prospective) subjects, so for the reason of redemptive justice.

One can find a mission-related war theory in Saint Augustine[27] (354–430) and in the historical Hungarian idea of the Holy Crown.[28]

---

18 Isidore of Seville 2006: 365.
19 Isidore of Seville 2018: III. 48.11. 200.
20 Isidore of Seville 2018: III.48.11. 200.
21 Isidore of Seville 1966: 15.
22 Gerics 1980: 118.
23 Isidore of Seville 2018: 210.
24 Isidore of Seville 2018: I.2.5. 39.
25 Isidore of Seville 2018: I.2.1a. 38.
26 Isidore of Seville 1966: 15.
27 Boda 2020: 1689–1692; Weithman 2001: 234–252; Luban 2011: 10–15.
28 Boda 2021b: 269–280.

According to Saint Augustine, just war should be started and waged against the heretics and the sinners in general, because this sort of war is well-suited to God's intention of redemption. God's intention includes a particular plan for redemption, which should be mirrored by the intention of Christian participants of war and has to be conceived as a Christian mission for spreading redemption.

Saint Augustine considers happiness as the basic purpose of humans. Happiness, however, cannot be reached in the earthly world because of the earthly sins and original sin in general, but only in the afterlife with the help of redemption by God. Such happiness means living forever in spiritual (and celestial) peace.[29] Redemption of humanity is not a unique deed of God, but an uncovering series of events in history.[30] Wars are the characteristic features of history,[31] through which God wants[32] to bring the peace of redemption to humanity. The ways to redemption for those who live Christian (just and pious) life and for those who live a sinful life are different.

People loving God and living a Christian life are called the citizens of the 'City of God' *(civitas Dei)* by Saint Augustine, and they may count for redemption in a peaceful way. Redemption will supplement earthly life in this case and bring everlasting spiritual (and celestial) peace for them. Leading a life of this sort, however, is not easy, because sinners and their wars rule earthly world, as Saint Augustine calls it, the 'Earthly city' *(civitas terrena).*[33]

Sinners are those who lead their life selfishly, adversely, violently, cruelly and unmercifully, and they are motivated by power-mongering instead of loving of God; or those who promulgate their heretic ideas prevent the uncovering of God's redeeming plan. Redemption, however, is not denied from sinners. They can reach it if they let themselves to be persuaded by arguments and abandon their sinful activity. If not, then they can attain redemption with the help of violent or even deadly punishment. According to Saint Augustine, punishment is a feasible method to change convictions and purify the soul of the sinners as oral persuasion, even it results the death of the sinners' body and to reach redemption.[34] This is the clearest form of redemptive justice.

The theory of Saint Augustine focuses on redemption, afterlife peace and happiness, and represents an offensive form of mission-related theories. The Crusades were good examples for the application of this theory.[35] In contrast, just war thinking based on the Hungarian idea of the Holy Crown connects happiness to the earthly 'redemption', to living on a particular territory. The theory also links warfare justice to the defence of this territory and the country situated on it, to secure the happiness of the country, and to punish the peacebreakers of the unity of the country. Hence just war thinking based on the Hungarian idea of the Holy Crown also includes redemptive justice.

---

29 Augustine 2000: XIX. 11.
30 Augustine 2000: XV. 1.
31 Augustine 2000: XV. 4.
32 Augustine 2000: XXII. 2.
33 Augustine 2000: XV. 1–4.
34 Augustine 1886: Chapter 14. 485.
35 Cushing 1995: 359–360; Riley-Smith 2005: 52–53.

The idea of the Holy Crown was developing between the 14–20th centuries, and its basic element is the reference to the historical Hungarian crowning device – the Holy Crown –, and to its two important features, its holiness and territorial connotation. The Holy Crown was respected and applied in crowning ceremonies as the crown of the Hungarian state founder King Saint Stephen I (975–1038) for centuries, last time in 1916. According to the Catholic tradition, King Stephen asked a crown from Pope Sylvester II at the very beginning of the 11th century, and the pope gave it to the king because a messenger of God had advised so in his dream. Therefore, the origin of the holiness of the crown is the God-given feature of it. However, it is linked to the Hungarian saint kings, Stephen I and Ladislaus I (1046–1095) also, and in the 12th century the crown was referred to as 'the crown of the saint kings'. Finally, because of its 'saint kings'-related nature, the crown earned a territorial connotation as well. It meant to refer to the territory of the Medieval Hungarian Kingdom. Stephen and Ladislaus were the kings who conquered, stabilised and organised the core territories of the Hungarian Kingdom.

Just war thinking based on the idea of the Holy Crown is a right intention-related theory, which includes a mission to secure the peace, stability and happiness on the territory of the Hungarian Kingdom. One of the important representatives of the theory is Péter Révay (1568–1622).[36] Révay dealt with the history of the Holy Crown and linked it to the civil wars of Hungary. According to Révay, the Holy Crown is not only holy in its origin, but It is Godly in Its nature, because It includes the Godly Providence, which is taking care – through the king – of Hungary and its members. The Godliness of the Crown grounds its highness, which results in the authority and honour of the properly crowned king and the liberty of the crowing nobility; who (together) in turn manage the happiness of the country with the help of their laws.

If the king is power-monger or the nobility is divided, then the Crown emigrates from the country (i.e. an unaccordant person from the ruling dynasty takes it abroad), and the king does not serve the happiness of the country. The result is civil war between the members of the ruling dynasty, or the parties of the nobility. According to Révay, civil war is a sin against God, hurts the highness of the Crown and causes unlawful situation. The Crown, and of course the properly crowned king who applies it to his holy and just aims, punishes the peacebreakers and separatists, restores the unified condition of the country and secures happiness. As Révay puts it: "Because finally with the support of the Holy Crown the true case of the kings comes to win. Those princes to whom the God judges lordship and who at the same time are meek, pious, true, and are taking care of their subjects, such kings are always protected by the Heavenly creatures, and finally escape from any trouble and danger."[37] Révay's examples for these kings are Charles (Angevin) I (1308–1342), Matthias (Corvinus) I (1458–1490), who made peace among the families, or the parties of the nobility, and Matthias (Habsburg) II (1557–1619) who – in the lifetime of Révay – brought peace between Christian denominations.

[36] Révay 1979: 195–232.
[37] Révay 1979: 203.

Just cause

According to the just cause-related forms of just war thinking, justice of war depends on whether the warring party has a just cause before of the war, or not. Right intention defines a sort of 'cause' as well, but it differs from just cause. Just cause articulates an aim, which can be reached in the near future, and right intention defines a more remote purpose. We can discern three main types of just cause-related just war thinking: when the state or the leader of the community (in the Middle Ages the prince) wages just war for enforcing law, maintaining Christian peace, and attaining punishment; when two conflicting or even warring states act equally demanding their causes are just and they (or one of them) regard the laws of conduct in warfare also; finally, when revolutionaries wage just war against the state (or the leader of the state).

Just war as enforcing the laws of the community of Christians

We have met the general points of the theory of Saint Thomas Aquinas in a previous section. I have been using these basic points to show the different forms of just war thinking. Saint Thomas Aquinas, however, developed a particular just cause-related theory as well.[38] According to him:

- the most important character of just war is its cause, because
- it is morally permissible to wage war against people or a country which deserves punishment for the previously committed injustice
- punishment is a form of corrective justice which means in this case enforcing human law
- enforcing the law is the duty and obligation of the prince in order to maintain Christian peace

Several thinkers before Saint Thomas Aquinas conceived just war as punishment, one of them was Saint Augustine, who linked the concept of punishment to his more basic concept of redemption. These thinkers had a quite different theory on the standards of implementing punishment. They typically linked this standard to the will, the order, or the judgement of God. Saint Thomas Aquinas, in harmony with his recognition and acknowledgment of natural characteristics of men, claims human laws are dependent on natural laws. He thinks natural laws define what is just or unjust, and hence that justice regarding the starting of a war depends on natural laws. The first and most important law of nature is that "good is to be done and pursued, and evil is to be avoided", a case of which is that "human life should be secured".[39] In connection with war Saint Thomas Aquinas holds that "a just cause is required, namely that those who are attacked, should be attacked because they deserve it on account of some fault (*culpa*)".[40]

---

38 Boda 2022a: 172–175; Reichberg 2018: 17–41.
39 Aquinói Szent Tamás 2011: q. 94/2. 31.
40 Aquinas 2013b: 177.

Committing a fault is to violate the human law, which is framed as the rule of all human acts, and purpose of the common good. Human law has two forms, the civil law of the state and the law of the nations. Further, human law is a form of positive law, which in turn is the declared form of natural law, which, again, is the rational aspect of the eternal law (in fact plan and wisdom) of God.[41] Because of the relationships of the different types of laws violating human laws (whether the civil law of the state or the law of the nations) it is violating the eternal law. Likewise, enforcing human law (whether the civil law of the state or the law of the nations) is not other than enforcing the eternal law of God. Just cause of war is violating unjustly human law (whether the law of the state or the law of the nations) which deserves punishment and correction in order to enforce the law. This is the clearest case of corrective justice.

According to Saint Thomas Aquinas punishment of injustice should be initiated by the sovereign prince, so he has legitimate authority. This is a right and an obligation of the prince, which originates from the fact that he is the leader of the community, so he has the right and duty to secure the common good of the community, to protect the community against invaders, and to maintain the social order of the community against crime.[42]

This right and duty of the prince implies that the prince's reflection to injustice should propose the general aim of maintaining the peace of the Christian community. Peace was an important Christian concept already before Saint Thomas Aquinas, for example in Saint Augustine. The previous conception, however, conceived peace spiritually, as the God secured harmony between the desires of a man, which can be reached completely only in the Heavens. Saint Thomas Aquinas takes peace partly as earthly and naturally occurred harmony between the members of Christian community.[43]

Just war as revolution against the oppressive and exploitative state

The second just cause-related theory is the communist theory of the revolutionary war, according to which the just cause is the oppression and exploitation of the class of proletariat by the state leader class of bourgeoisie.[44] In details:

- the just cause is the bourgeois state oppression and exploitation and so distributive injustice
- the oppressed people are morally permitted to start a revolutionary war for the elimination of the class of bourgeois and the state as its representative
- revolution terminates oppression and exploitation inside the society and all over the world

One prominent representative of the communist just war theory is Vladimir Ilych Lenin (1870–1924). According to Lenin bourgeois oppression of the proletariat should be

41 Aquinói Szent Tamás 2011: q. 90–96. 3–53.
42 Aquinas 1997: I. 3. 65–67.
43 Aquinas 2013a: 174.
44 Ryder 2019: 31–44.

terminated and what makes attainable this purpose is the war between the bourgeois class and the proletariat only. As Lenin puts it: "We fully regard civil wars, i.e., wars waged by the oppressed class against the oppressing class, slaves against slave-owners, serfs against land-owners, and wage-workers against the bourgeoisie, as legitimate, progressive and necessary."[45]

Erich Wollenberg (1892–1973), the Russian–German communist thinker between the world wars, lists four different just causes among the different forms of oppression which justifies war. War is just if it is the revolutionary war of the proletariat against the oppressor, or against a foreign aggressor who supports the oppressor, or against counterrevolutionaries who are supported by foreign aggressors; further, if it is liberty war of the people of an oppressed colony against the oppressors.[46] The common point of all these wars is their just cause, the fight against the morally mistaken distribution of goods, exploitation and for the liberation and protection of the people. Revolutionaries ground their just cause to distributive injustice.

This cause is the suitable cause for those classes which suffer from the oppression, so the proletariat and the people of the colonies, and which is in the proper situation. The proper situation for revolution is defined by the developed social-economic conditions of the country, and particularly of the oppressed class. Hence war is the continuation of politics, and politics is the corollary of economic situation.[47] In this case other socialist countries, which already have fought successfully against their oppressors, are morally permitted to intervene into the revolution against oppression in another country. The revolution, however, cannot be exported arbitrarily.

The future purpose of communist just war, the right intention condition of the communist theory is to eliminate oppression all over the world. In the preferred future but yet during the war against the bourgeoisie, proletarian national states will persist and they come into the relation of equality with each other; after the victorious war, however, the proletarian state will be dying away because after the bourgeois class ceased to exist the proletarian will cease to exist too.[48]

Just war as regular war between states

Finally, the third just cause-related theory defines just war as a legally regulated contest between states.[49] In details:

- in contest both conflicting states have a (possibly) just cause for starting the war
- the war itself serves as the process of settling the conflict and to make decision about it
- conflicting states should conduct their war with regarding the rules of international law and so legal justice

[45] Lenin 1966: 4.
[46] Wollenberg 1936: 2–5.
[47] Lenin 1964a: 65.
[48] Lenin 1964b: 398–399.
[49] Kalmanovitz 2018: 145–165.

Two important representatives of this theory are Alberico Gentili (1552–1608) and Hugo Grotius (1583–1645).

According to Gentili "war is a just and public contest of arms"[50] between sovereign states, which is initiated by the leaders (princes) of states in necessity. In this case a superior judge does not exist who is entitled to make decision in a debate between sovereign states, and if the conflict demands some settlement and there is no time for negotiation and judicial argumentation, then the debate should be settled by war.[51] This sort of war is just on both sides, because it is possible that in the debate none of the debating parties take an unjust position. Since even if one or the other party seeks to draw a sincere moral judgement on the just or unjust nature of his war, it is possible that it does not possess all the relevant information to reach the sound conclusion. Further, in war both parties have just cause if they go to war for any sound reason and aim at justice at the same time. This is because going to war without sound reasons is neither just war nor war but brigandage. Finally, it is possible that one side is just, but the other one is more just, because one side does not cease to be just because of his opponent has more just case.[52]

Gentili claims that just war appears in the state of necessity and for the reason of protecting the state. This condition seems at first sight to be a restrictive one; however, in the theory of Gentili it works in quite the opposite manner. Gentili lists several different causes of just war, from which some come from the human nature and in this sense, they are necessary and protective. These causes are self-defence in actual danger, defence in fear that one may himself be attacked, and honourable defence of others based on any association with them (e.g. kinship, love, kindliness, human fellowship).[53]

Similarly to Gentili, Hugo Grotius also holds a theory of war as a contest which he calls regular war *(bellum solenne)* (besides this theory he holds a theory based on law enforcement and punishment as well [*bellum iustum*][54]). The origin of regular war theory is those past situations which involved a debate between states but in which the outsider states could not make a clear judgement on the justness of the claims and on the right range of reactions. If outsider states had made judgement in these situations they would have got involved in the debate.[55] For this reason they entrusted the decision in debate to the states and to the Laws of Nations.[56]

According to Grotius: "Two Things then are requisite to make a War solemn [regular] by the Law of Nations. First, that it be made on both Sides, by the Authority of those that have the Sovereign Power in the State: And then, that it be accompanied with some Formalities".[57] This means that war should be started by that person who possesses the legitimate authority, who represents the sovereignty of the state, and should be waged by respecting the international legal rules of conduct in war. The most important such

50 Gentili 1933: I–II. 12.
51 Gentili 1933: I–II–III. 12–21.
52 Gentili 1933: I. VI. 31–33.
53 Gentili 1933: I. XIII. 58–73.
54 Grotius 2005b: I. II. 1–2. 393–395.
55 Grotius 2005c: IV. IV. 1275–1277.
56 Grotius 2005a: III. IV. 1. 248.
57 Grotius 2005a: III. IV. 1. 250.

rule is the rule of declaration of war, which shows the war begun by the possessor of the legitimate authority. By the declaration the state lets the other party (and the allies and members of his own state) know that the declarator is legally at the state of war with him. Declaration also changes the range of the valid legal rules, so it connects legal effects to the state of war, so the declaration separates state of war from state of peace before the war (like the peace treaty at the end of war).[58]

Summary and conclusion: Forms of justice and forms of historical just war thinking

I overviewed five forms of historical just war thinking, the theory of judgement of God, the mission-related just war thinking, the law-enforcing theory, the revolutionary theory and the regular theory. I classified these theories with the help of the main concepts of Saint Thomas Aquinas's just war theory. Now I match them to the main concepts of justice I mentioned at the beginning of the article.

Hence, the theory of the judgement of God holding that just wars are wars which started by God, judged as just by God, and brought about being victorious by God. This theory so emphasises legitimate authority of God and the procedural justice of God's judgement. The mission-related form of just war thinking sees right intention and remote aims to be important, and focuses on helping the needy and for this reason redemptive justice. The law-enforcing, the revolutionary and the regular theory similarly hold essential just cause; however, the law-enforcing theory includes punishment and corrective justice, the revolutionary theory contains in reference to exploitation and so distributive justice, and finally the regular theory secures just cause for both warring parties and introduces the legal justice of international law.

This classification shows that historical just war thinking did not have a simple frame and a simple history starting from Saint Augustine or the Roman or Greek Antiquity. Just war thinking in its every form should refer to some forms of justice, however, as many concepts of justice occurred, many forms of just war thinking appeared. This is a process which did not end up with the revolutionary theory. After the Second World War, a new form of just war thinking turned up. Michael Walzer claims just cause is the most important part of the theory, in which justice is the protection of the rights of the communities against injustice and violation. This form of just war thinking is like the law-enforcing model, with the difference that the law-enforcing model stresses punishment but Walzer claims protection of rights as the basic tenet of just war theory.

References

Aquinas, Thomas (1997): *On the Government of the Rulers. De Regimine Principium.* Philadelphia: University of Pennsylvania Press.

[58] Grotius 2005c: III. 1246–1269.

Aquinas, Thomas (2013a): Summa Theologiae II–II. Question 29: On Peace. In Reichberg, Gregory M. – Syse, Henrik – Begby, Endre (eds.): *The Ethics of War. Classic and Contemporary Readings.* Malden, MA – Oxford – Carlton, Victoria: Blackwell Publishing. 171–176.

Aquinas, Thomas (2013b): Summa Theologiae II–II. Question 40: On War. In Reichberg, Gregory M. – Syse, Henrik – Begby, Endre (eds.): *The Ethics of War. Classic and Contemporary Readings.* Malden, MA – Oxford – Carlton, Victoria: Blackwell Publishing. 171–182.

Aquinói Szent Tamás [Thomas Aquinas] (2011): Summa Theologica. In Aquinói Szent Tamás [Thomas Aquinas]: *A* Summa Theologiae *kérdései a jogról* [Summa Theologiae on Law]. Budapest: Szent István Társulat.

Aristotle (2004): *Nicomachean Ethics.* Translated by Roger Crisp. Cambridge: Cambridge University Press.

Augustine, Saint (1886): Letter 138 (To Marcellinus). In Schaff, Philip (ed.): *Nicene and Post-Nicene Fathers of the Christian Church I.* Buffalo: The Christian Literature Company.

Augustine, Saint (2000): *The City of God.* Translated by Marcus Dods. New York: Modern Library.

Bobocel, D. Ramona – Gosse, Leanne (2015): Procedural Justice: A Historical Review and Critical Analysis. In Cropanzano, Russell S. – Ambrose, Maureen L. (eds.): *The Oxford Handbook of Justice in the Workplace.* Oxford: Oxford University Press. 51–88. Online: https://doi.org/10.1093/oxfordhb/9780199981410.001.0001

Boda, Mihály (2020): Az igazságos haború hagyománya Európában és a Távol Keleten (Kínában) [Just War Tradition in Europe and the Far East (China)]. In Pohl, Árpád (ed.): *Biztonság és honvédelem.* Budapest: Ludovika Egyetemi Kiadó. 1689–1701.

Boda, Mihály (2021a): Háborús ideológiák a középkori Magyarországon: istenítéleti ideológia, az igazságos háború elmélete [Warfare Ideologies in Medieval Hungary: Ideology of Judgement of God, Just War Theory]. *Hadtudomány,* 31(1), 62–74. Online: https://doi.org/10.17047/HADTUD.2021.31.1.62

Boda, Mihály (2021b): Hungarian Theory of Just War Based on the Idea of the Holy Crown: A Historical Case of Just Mission. *Journal of Military Ethics,* 20(3–4), 269–280. Online: https://doi.org/10.1080/15027570.2021.2018797

Boda, Mihály (2022a): Az igazságos háború elméletének kiterjesztése a rendészetre: történelmi és kortárs elméletek. Az igazságos rendészet elmélete [Applying Just War Theory for Policing: Historical and Contemporary Theories. Just Policing Theory]. *Belügyi Szemle,* 70(1), 169–185. Online: https://doi.org/10.38146/BSZ.2022.1.10

Boda, Mihály (2022b): *The Warfare Ideology of Ordeal: Another Form of Just War Thinking? Theory and Practice from the Early Middle Ages.* Online: http://real.mtak.hu/129507/1/Boda_Warfare%20Ideology%20of%20Ordeal_Lek_20210507.pdf

Cushing, Kathleen G. (1995): Anselm of Lucca and the Doctrine of Coercion: The Legal Impact of the Schism of 1080? *The Catholic Historical Review,* 81(3), 353–371. Online: https://doi.org/10.1353/cat.1995.0031

Frowe, Helen (2011): *The Ethics of War and Peace. An Introduction.* London – New York: Routledge.

Gentili, Alberico (1933): *De Iure Belli. Libri Tres.* Vol. 1–2. Volume 2 translated by John C. Rolfe. Oxford–London: The Clarendon Press – Humphrey Milford.

Gerics, József (1980): Judicium Dei a magyar állam XI. századi külkapcsolataiban [Iudicum Dei in the Hungarian State's Foreign Relations in the 11th Century]. In Mezey, László (ed.): *Athleta Patriae – Tanulmányok Szent László történetéhez* [Athleta Patriae – Essays on the History of Saint Ladislaus]. Budapest: Szent István Társulat. 111–134.

Gratian (2013): Decretum, part II, causa 23. In Reichberg, Gregory M. – Syse, Henrik – Begby, Endre (eds.): *The Ethics of War. Classic and Contemporary Readings.* Malden, MA – Oxford – Carlton, Victoria: Blackwell Publishing. 109–124.

Grotius, Hugo (2005a): *The Rights of War and Peace. Book I.* Indianapolis. Liberty Fund.

Grotius, Hugo (2005b): *The Rights of War and Peace. Book II.* Indianapolis: Liberty Fund.

Grotius, Hugo (2005c): *The Rights of War and Peace. Book III.* Indianapolis: Liberty Fund.

Isidore of Seville (1966): History of the Kings of Goths. In *Isidore of Seville's History of the Kings of the Goths, Vandals, and Suevis.* Translated by Guido Donini – Gordon B. Ford Jr. Leiden: E. J. Brill. 3–33.

Isidore of Seville (2006): *The Etymologies.* Cambridge: Cambridge University Press.

Isidore of Seville (2018): *Sententiae.* Translated by Thomas L. Knoebel. New York – Mahwah, NJ: The Newman Press.

Johnson, James Turner (2006): The Just War Idea: The State of the Question. *Social Philosophy and Policy,* 23(1), 167–195. Online: https://doi.org/10.1017/S0265052506060079

Kalmanovitz, Pablo (2018): Early Modern Sources of the Regular War Tradition. In Lazar, Seth – Frowe, Helen (eds.): *The Oxford Handbook of Ethics of War.* Oxford: Oxford University Press. 145–165.

Lenin, Vladimir Ilych (1964a): The Tasks of the Proletariat in our Revolution. In *Lenin Collected Works. Volume 24 (April–June 1917).* London: Lawrence and Wishart, Moscow: Progress Publishers. 57–91.

Lenin, Vladimir Ilych (1964b): War and Revolution. *Lenin Collected Works. Volume 24 (April–June 1917).* London: Lawrence and Wishart, Moscow: Progress Publishers. 398–421.

Lenin, Vladimir Ilych (1966): The Principles of Socialism and the War of 1914–1915. In *Lenin on the War and Peace. Three Articles.* Beijing: Foreign Languages Press. 4–57.

Luban, David (2011): War as Punishment. *Georgetown Law Faculty Working Papers,* (145), 11–71. Online: https://scholarship.law.georgetown.edu/fwps_papers/145/

McMahan, Jeff – McKim, Robert (1993): The Just War and the Gulf War. *Canadian Journal of Philosophy,* 23(4), 501–541. Online: https://doi.org/10.1080/00455091.1993.10717333

Mille, David (2021): Justice. In Zalta, Edward N. (ed.): *The Stanford Encyclopedia of Philosophy.* 2021. Online: https://plato.stanford.edu/archives/fall2021/entries/justice/

Ramsey, Paul (1978): *Basic Christian Ethics (Midway reprint).* Chicago–London: The University of Chicago Press.

Rawls, John (1999): *Theory of Justice.* Cambridge, Mass.: The Belknap Press of Harvard University Press.

Reichberg, Gregory M. (2018): *Thomas Aquinas on War and Peace.* Cambridge: Cambridge University Press. 17–41.

Révay, Péter (1979): Révay Péter Turóc vármegyei főispán emlékirata Magyarország több mint 600 éve tündöklő Szent Koronájának eredetéről, jeles és győzedelmes voltáról, sorsáról. In Katona, Tamás (ed.): *A korona kilenc évszázada.* Budapest: Magyar Helikon. 195–232.

Riley-Smith, Jonathan (2005): Crusading as an Act of Love. In Berman, Constance H. (ed.): *Medieval Religion. New Approaches.* New York – London: Routledge. 44–60. Online: https://doi.org/10.4324/9780203328675_chapter_2

Ryder, Andrew (2019): "The only Justifiable War" The Marxist Strategies of Lenin, Trotsky, and Blanco. An Introduction to International Perspectives. In Cordeiro-Rodrigues, Luís – Singh, Danny (eds.): *Comparative Just War Theory.* Lanham – New York – London: Rowman and Littlefield. 31–44.

Walzer, Michael (1992): *Just and Unjust Wars.* New York: Basic Books.

Weithman, Paul (2001): Augustine's Political Philosophy. In Stump, Eleonore – Kretzmann, Norman (eds.): *The Cambridge Companion to Augustine.* Cambridge: Cambridge University Press. 234–252. Online: https://doi.org/10.1017/CCOL0521650186.017

Wollenberg, Erich (1936): Just Wars in the Light of Marxism. *New International,* 3(1), 2–5.

AARMS Vol. 22, No. 1 (2023) 77–90.

10.32565/aarms.2023.1.6

Certain Characteristics of Strategic Communication in Armed Conflicts over the Past Decades

Péter TORDA[1]

This article argues a discrepancy between the low degree of interest afforded to military disciplines in strategic communication research and the high degree of significance of strategic communication to modern military practice. A relatively low number of scholarly articles have been published in the field of strategic communication which focus on military disciplines, with most of them being empirical studies addressing research objects on the frontiers of military science. Meanwhile, strategic communication has become increasingly central to military practice in the post-1990 period, as seen in armed conflicts in Iraq, Afghanistan and Ukraine.

Keywords: *strategic communication, military science, military practice, armed conflict, modern warfare*

Introduction

In the past decades, we have seen a *boom* in strategic communication, both as a "global field of communication research"[2] and as a line of practice. Even though the very concept of strategy originates from military theory[3] and strategic communication has firm roots in the military domain,[4] military science and its disciplines seem to have had limited impact on the evolution of strategic communication as a discipline. This assumed insufficiency of attention afforded to military science in strategic communication scholarship stands in contrast with the assumption of a steadily growing significance of strategic communication as part of military practice in armed conflicts over the past decades.

[1] PhD student, University of Public Service, Doctoral School of Military Sciences, e-mail: torda.peter@stud.uni-nke.hu

[2] Nothhaft et al. 2018a: 329.

[3] Nothhaft–Schölzel 2015: 18–33.

[4] Németh 2021a: 17.

Hypotheses and methodology

To analyse the evolving nexus of strategic communication, military science and armed conflict in the past thirty years, I am proposing two hypotheses:

H1: The perspective and objects of military science are largely absent from research on strategic communication.

H2: Strategic communication as a practice has become increasingly central to armed conflicts since the beginning of the 1990s.

To prove or disprove the above hypotheses, I have applied the method of literature review and content analysis.

To explore the integration of military disciplines into strategic communication research (H1), I performed a full-text search using the term "military" in the International Journal of Strategic Communication (IJSC) as well as the Routledge Handbook of Strategic Communication (RHSC).[5]

> While the work published in IJSC is not a complete representation of strategic communication research production, it is the only academic journal in the world dedicated to strategic communication. In addition, IJSC provides the only continuously produced academic source from which to draw longitudinal data regarding the breadth and scope of scholarship in strategic communication.[6]

The RHSC is the most complete edited volume to aggregate knowledge from strategic communication research.

To analyse the integration of strategic communication as a practice in the military domain through recent decades (H2), I reviewed literature in those three online databases of the Library of the University of Public Service which contained the highest combined number of publications indexed in the research fields of security studies and military science:[7] the Oxford Academic Journals, the Taylor and Francis Online and the JSTOR databases. I performed full-text searches and follow-up snowball searches using relevant terms.[8]

---

5 Holtzhausen–Zerfass 2015.

6 Page Werder et al. 2018: 347.

7 As of 3 May 2021 (www.uni-nke.hu/konyvtar/adatbazis-ajanlok/kutatasi-terulethez-javasolt-adatbazisok).

8 The following search terms were used: "Gulf War" and "Iraq" and "strategic communication"; "Iraq" and "invasion" and "strategic communication"; "Iraq" and "war" and "strategic communication"; "Afghanistan" and "war" and "strategic communication"; "global war on terror" and "strategic communication"; "ISIS" and "strategic communication"; "Russia" and "Ukraine" and "strategic communication"; "Russia" and "Crimea" and "strategic communication".

Defining strategic communication: Communication scholarship and military conceptualisation

Before moving on to examining the hypotheses proposed in this article, it is necessary to outline the contours of the concept of strategic communication, both from the perspective of communication and of military science.

From the viewpoint of strategic communication research, the seminal definition describes the concept as "the purposeful use of communication by an organization to fulfill its mission".[9] Synthetising the results of a decade of subsequent research in the field, a more elaborate definition of strategic communication has been proposed to "encompass all communication that is substantial for the survival and sustained success of an entity. Specifically, strategic communication is the purposeful use of communication by an organization or other entity to engage in conversations of strategic significance to its goals".[10]

However, and notwithstanding the explanatory power of these definitions, strategic communication has been described as an "emerging interdisciplinary paradigm"[11] and an "elusive concept".[12] There is broad agreement among scholars about the integrated and interdisciplinary[13] nature of strategic communication, with "interdisciplinary integration representing the greatest challenge for strategic communication scholarship in the future".[14] Different variations have been put forward to identify the root disciplines unified by the progressively growing body of knowledge on strategic communication. A non-exhaustive list of constitutive disciplines associated with strategic communication includes management, marketing, public relations, technical communication, political communication and information/social marketing campaigns,[15] advertising, corporate communication, organisational communication,[16] health and intercultural communication,[17] as well as communication and media science.[18] Furthermore, disciplines which seek scientific and technological answers to the subject matter of strategic communication have been added to the list of root disciplines, including computer linguistics, data science, cognitive science and neurobiology.[19]

As regards the conceptualisation of strategic communication in the (Western) military domain, the Military Concept for NATO Strategic Communication states that:

> All aspects of the Western military alliance's activities have a critical information and communications component. This concept proposes that strategic communications is not an

9 Hallahan et al. 2007: 3.
10 Zerfass et al. 2018: 493.
11 Page Werder et al. 2018: 333–351.
12 Nothhaft et al. 2018b: 352–366.
13 Page Werder et al. 2018: 347.
14 Page Werder et al. 2018: 349.
15 Hallahan et al. 2007: 3.
16 O'Connor–Shumate 2018: 399.
17 Nothhaft et al. 2018a: op. cit. 329.
18 Nothhaft et al. 2018b: op. cit. 355.
19 Nothhaft et al. 2018b: op. cit. 356.

> adjunct activity, but should be inherent in the planning and conduct of all military operations and activities. As part of the overarchlng [sic!] political-military approach to Strategic Communications within NATO, the vision is to put Strategic Communications at the heart of all levels of military policy, planning and execution, and then, as a fully integrated part of the overall effort, ensure the development of a practical, effective strategy that makes a real contribution to success. […] In accordance with NATO Policy, NATO Strategic Communications is the coordinated and appropriate use of NATO communications activities and capabilities Public Diplomacy, Public Affairs (PA), Military Public Affairs, Information Operations (Info Ops) and Psychological Operations (PsyOps), as appropriate – in support of alliance policies, operations and activities, and in order to advance NATO's aims.[20]

One of the salient questions in conceptualising strategic communication in the military field relates to which types of actions are considered to constitute strategic communication. In certain interpretations, "not only messages or communicative interactions belong to strategic communication, but also the actions of people, because they also communicate, and consequently constitute organizational life as such and thus constitute strategy".[21] Accordingly, it has been argued from a military scholarly standpoint that strategic communication "should not be limited to formal messages, while actions also convey meaning and should, therefore, also be part of strategic communication. What we do is often more important than what we say".[22] The notion that people's actions in organisations may also amount to strategic communication takes on a special meaning in the military context where individual actions may easily become matters of life and death. The concept of the *era of the strategic corporal*[23] is one reflection of this viewpoint.

Integrating military science into strategic communication research

A full-text search using the term "military" in the IJSC lists 56 manuscripts published over the 2007–2022 period, while the same search lists 10 manuscripts published in the RHSC. This is out of a total of 354 manuscripts published in the IJSC in the period 2007–2022, while the RHSC contains 38 publications overall.

Content analysis of the International Journal of Strategic Communication

Forty-seven of the 56 articles listed in the IJSC do not have their disciplinary focus anchored in military science. However, some of these publications contain references to

[20] NATO: Military concept for NATO strategic communication (https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf cited in Zerfass et al. 2018: 489).
[21] Van Ruler 2018: 376.
[22] Paul 2011: 28 cited in Van Ruler 2018: 373.
[23] Németh 2021b: 130.

research objects in the military domain. In the very first issue of the IJSC, it is stated that "the U.S. government recognizes strategic communication as a critical element in public diplomacy and in military intervention in troubled areas such as Iraq and Afghanistan".[24] And, in another reference to the military domain in the same article, it is posited that strategic communication research "can be informed by looking beyond the bounds of traditional communications disciplines to include such diverse activities as public diplomacy, psychological operations by the military, and social marketing".[25] More detailed references are made to objects of military research in a 2018 article, which states that "there is an old but increasing interest in communication in the context of military and national power".[26] It goes on to state that:

> Interestingly, strategic communication as an integral element of warfare is widely neglected by communication science, probably due to the negative notions of information warfare and propaganda. However, it has gained new attention in the context of terrorism and counterterrorism […] The same is true for public diplomacy as a more "civilized" way of exercising soft power through global and intercultural communication. These topics resonate well in communication science […] and show first signs of an institutionalization of their own. […] In the real world, those practices are closely connected to military communication.[27]

Another article in the IJSC, with a disciplinary focus on evolutionary psychology, confirms the finding that "military organizations are not the prime concern of strategic communication research".[28]

Nine of the 56 articles listed in the IJSC are rooted in military science: a) Becoming a "Normal" and "Ordinary" Organization through Strategic Communication? Discursive Legitimation of the Swedish Armed Forces;[29] b) Military Perspective on Strategic Communications as the "New Kid on the Block": Narrating the Czech Military Deployment in Afghanistan and the Baltic States;[30] c) Is *IS* Online Chatter Just Noise?: An Analysis of the Islamic State Strategic Communications;[31] d) A Lack of Effect Studies and of Effects: The Use of Strategic Communication in the Military Domain;[32] e) Country Image Repair Strategies During an Asymmetrical Conflict: An Analysis of the Gaza Conflict in 2014;[33] f) A Terrorist Group's Strategic Communication – The Case of the Red Army Faction;[34] g) Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods;[35] h) Propaganda's Place in Strategic Communication: The

---

24 Hallahan et al. 2007: 8.
25 Hallahan et al. 2007: 27.
26 Zerfass et al. 2018: 489.
27 Zerfass et al. 2018: 489–490.
28 Seiffert-Brockmann 2018: 425.
29 Ågren–Sataoen 2022: 50–69.
30 Vyklický–Divišová 2021: 231–252.
31 Royo-Vela–McBee 2020: 179–202.
32 Wallenius–Nilsson 2019: 404–417.
33 Tabak–Avraham 2018: 237–251.
34 Rothenberger 2017: 286–305.
35 Magen 2017: 269–285.

Case of ISIL's Dabiq Magazine;[36] i) "My God is Not Your God": Applying Relationship Management Theory to Managing Ethnoreligious Crises in Sub-Saharan Africa.[37]

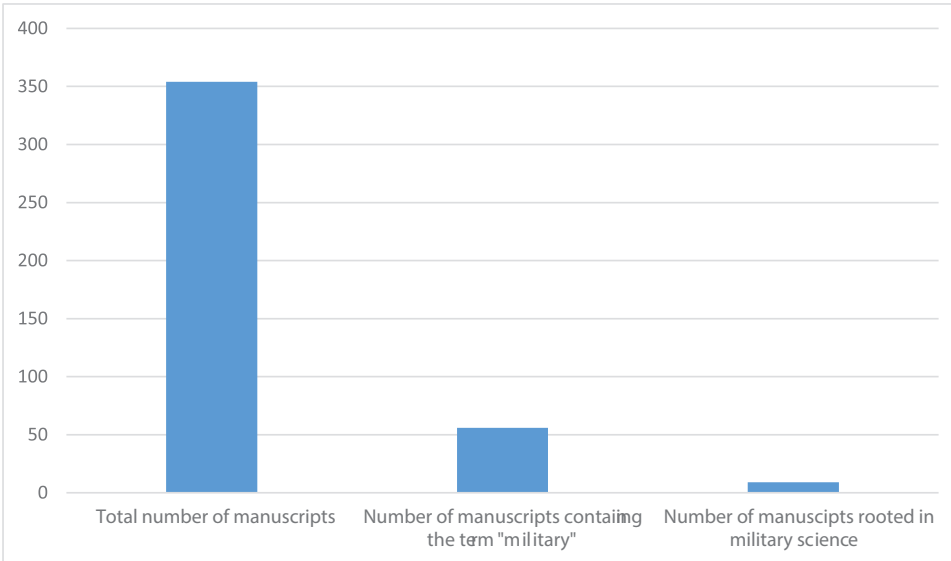

Figure 1: Content analysis of the IJSC (2007–2022)

Source: Compiled by the author.

Content analysis of the Routledge Handbook of Strategic Communication

Nine of the 10 publications listed in the RHSC do not have their disciplinary focus anchored in military science. However, one among these publications[38] references research objects in the military domain, namely case studies conducted with two U.S. military units to analyse different aspects of the institutionalisation of public relations in entities which practice strategic communication.

One publication was found in the RHSC with a clear foundation in military science: (Re-)Reading Clausewitz: The Strategy Discourse and its Implications for Strategic Communication.[39] This is a theoretical work, which intends to fill a gap in strategic communication scholarship when it comes to the study of classics of military science. It deconstructs the meaning of *strategy* in the Clausewitzian sense, with a view to "clarifying the concept of *strategic* in strategic communication".[40]

---

36 Wilbur 2017: 209–223.
37 Pratt – Azuka Omenugha 2014: 100–125.
38 Wakefield et al. 2015: 353–369.
39 Nothhaft–Schölzel 2015.
40 Nothhaft–Schölzel 2015: 19.

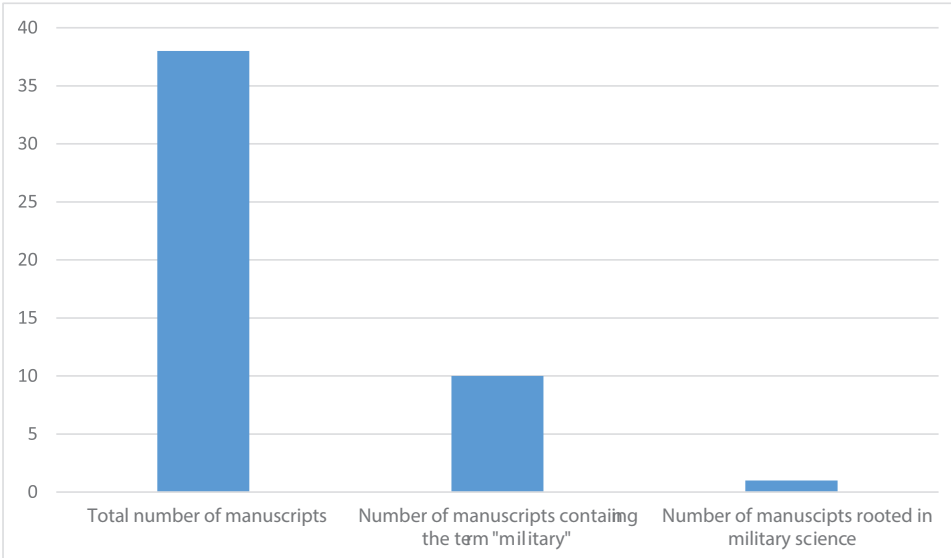

Figure 2: Content analysis of the RHSC

Source: Compiled by the author.

Conclusions

In conclusion, the content analysis conducted by the author reveals a low degree of integration of military science into strategic communication research. Most of the publications which actually focus on military disciplines address research objects on the frontiers of military science, namely military crisis management, (counter)terrorism and intelligence. There are three publications which concentrate on more mainstream military disciplines: strategic studies, psychological operations and military public affairs respectively. Further, the review exposed a tilt towards empirical studies: 6 empirical studies against 1 conceptual work and 3 hybrid works of a partly empirical and partly conceptual nature.

Strategic communication in armed conflicts over the past decades

On the basis of the assumptions and definitions introduced in the previous sections, instances of strategic communication as part of military practice are observable from the age of antiquity[41] through the present days.

[41] Németh 2021a: 36–67.

Against this background, the author proposes the hypothesis that the beginning of the 1990s represents a turning point, whereupon strategic communication has become increasingly central to armed conflicts and military efforts.

The diversifying nature of armed conflict in the past decades has been described through various concepts, such as small wars, asymmetric warfare, counterinsurgency operations, fourth generation warfare,[42] Revolution in Military Affairs, network-centric warfare, effects-based operations[43] and hybrid warfare. As local conflicts and peace operations multiplied worldwide, the concept of civil–military relations has been institutionalised in military organisations.[44] A connecting tissue across these concepts is the prominent role attributed to communication strategies.[45]

The following sub-sections will discuss in more detail certain examples from the post-1990 period for strategic communication in the context of armed conflicts, and will provide possible explanations for the trends and drivers that determined strategic communication in these settings.

The Gulf War of 1990–1991

The Gulf War took place at a confluence of technological breakthroughs in warfighting capacities and in global communication. "The novel employment of precision guided munitions and the technical capability to cover combat real-time via the media had previously not been possible in war. This was the first conflict extensively covered "live"."[46] Real-time and globally accessible media coverage of armed conflict created an unprecedented format of meaning construction across the news media, public opinion, political decision-making and military decision-making. News media assumed an instantaneous influence over the formulation of decisions in warfighting, and military commanders had to engage directly with public opinion.[47] The oft-cited term *CNN effect* encapsulates "the idea that real-time communications technology could provoke major responses from domestic audiences and political elites to global events".[48] A visible example of the intertwining of media and military decision-making during the conflict was the emergence of the U.S. General Norman Schwarzkopf, the commander of the coalition forces, as a media celebrity.[49]

It is further argued that the U.S.-led coalition exploited to its strategic advantage the new media landscape through conducting an "unprecedented media management campaign […] to win the war on the home front".[50] Meanwhile, the coalition's overwhelming

---

42 Németh 2013: 131.
43 McMaster 2008: 19–20 cited in Németh 2021b: 129.
44 Németh 2021a: 67.
45 Németh 2020: 13.
46 Adamson 1997: 4.
47 Adamson 1997: 2.
48 Robinson 1999: 301.
49 Németh 2021a: 66.
50 Mallet 1997: 280.

superiority in psychological operations capacity was seen as a crucial success factor on the battlefield.[51]

The Global War on Terror: Iraq and Afghanistan

Following the 9/11 terror attacks, U.S. President Bush has embarked upon a Global War on Terror (GWOT), which came to entail two large-scale armed conflicts in Afghanistan and in Iraq. The GWOT has influenced the development of military theory and practice, including the role of strategic communication in the military domain.[52] The unfolding of the GWOT coincided with the emergence of the interrelated trends of the "digital revolution, new message contributors and one-to-one message platforms".[53] These trends had a determinant impact on the strategic communication efforts of all stakeholders in the context of GWOT.

The U.S. invasion of Iraq in 2003 and the subsequent war lends itself to important conclusions from a strategic communication point of view. It is argued that once the invasion has ended, and President Bush declared mission accomplished, the U.S. political and military leadership has lost its hegemony in dominating news and managing public opinion about the conflict.[54]

> Continuing combat action received more minutes of network television coverage [in the U.S. – comment by the author] in 2004 than the invasion and subsequent fighting did in 2003, helping to explain why casualties were such a constant presence in news stories throughout the period. Moreover, the combination of suicide terrorism and the Abu Ghraib scandal received almost as much attention as Iraqi reconstruction in 2004 (Tyndall Report Archive).[55]

From this perspective, bombings committed by the insurgents in Iraq should not only be seen as combat actions, but also as the purposeful and strategic use of communication to further the overall goals of these organisation. The increasing availability and affordability of mobile devices and Internet connection enabled the insurgents with a strategic capacity to mediate their actions and messages to, and create meaning with, key audiences: sponsors, supporters and potential recruits, enemies, adversaries, domestic and foreign publics. In the same manner, insurgents deliberately engaged with foreign journalists and media outlets to pursue their strategic goals.[56]

Contrary to the 1990–1991 war in Iraq, the U.S.-led coalition lost the strategic communication initiative, and the insurgents' communication efforts proved more effective in advancing their strategic goals than those of the Western militaries deployed to Iraq. This strategic communication superiority on the side of the insurgents has explanatory

---

51 Mallet 1997: 280–297.
52 Németh 2013: 129–130.
53 O'Connor–Shumate 2018: 401.
54 Patrick–Thrall 2007: 95–96.
55 Patrick–Thrall 2007: 108–109.
56 Garfield 2007: 22–32.

power with regard to the "dramatic and resounding drop in public support coverage [in the U.S. – comment by the author] for Bush's handling of the war in Iraq",[57] falling from a high point of 76% to less than 50% by the fall of 2003 eventually sinking as low as 35% by 2005.[58]

As the GWOT continued, with major armed conflicts persisting in Afghanistan and Iraq, militant groups and terrorist organisations engaged in the conflicts developed strategic communication activities of increasing scope and sophistication. In 2005, al-Qaeda Deputy Ayman al-Zawahiri wrote to al-Qaeda in Iraq (AQI) founder Abu Musab al-Zarqawi: "We are in a battle, and […] more than half of this battle is taking place in the battlefield of the media."[59]

The self-proclaimed Islamic State of Iraq and Syria (ISIS) waged a strategic communication campaign of "unparalleled scope and complexity".[60] Strategic communication went to the very essence of the ISIS phenomenon, not only in terms of advancing its strategic goals on the ground, but also in helping to project the threat posed by ISIS beyond the region,[61] through inspiring terrorist attacks abroad, spreading terrorist propaganda and attracting foreign terrorist fighters and financing. Research has pointed out the integration between ISIS strategic communication and kinetic operations. "The positive relationship between the IS territorial control and the quality of its media production reflect a shift in the IS operations. As the IS experiences territorial expansion and military success, the organization dedicates more resources from warfighting to governance and strategic communication warfare."[62]

As in the case of Iraq, the U.S.- and NATO-led military operations in Afghanistan failed to gain a strategic communication advantage over the adversary. "[T]he Taliban did not prevail just because they lied more or understood Afghans better, but because they applied principles of strategic communications in a manner that was beyond what their more sophisticated adversaries could manage."[63] In particular, the Taliban has effectively integrated communication activities with military actions and public service provision in furtherance of its strategic goals of toppling the Kabul-based government and expelling foreign forces.[64]

Russian interventions in Ukraine

Strategic communication – which in the Russian context is often synthetised into concepts such as information warfare, propaganda or psychological operations – infuses Russian military practice and theory. There is broad consensus that, beginning with the early

[57] Patrick–Thrall 2007: 96.
[58] Patrick–Thrall 2007: 113–114.
[59] Royo-Vela–McBee 2020: 182.
[60] Winter 2020: 38.
[61] Royo-Vela–McBee 2020.
[62] Sweeney et al. 2020: 481.
[63] Johnson 2018: 960.
[64] Johnson 2018: 961.

2000s,[65] information operations have become an increasingly important aspect of Russian military practice, intensifying around the war in Georgia in 2008 and culminating around the interventions against Ukraine in 2014 and in 2022. Psychological operations, in particular, are explicitly discussed in the present Russian military doctrine and military theoretical debate.[66]

Russia's disinformation campaign against Ukraine has been characterised by a commander in the U.S. military as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare".[67] And the annexation of Crimea "could be seen as a turning point in modern successful Russian military operations which exploited information influence and interference, considered the first contemporary Russian use of cyber warfare and information operations alongside conventional military activity".[68] Indeed, in his famous *Gerasimov doctrine* speech of 2013, Russia's Chief of General Staff, General Valery Gerasimov, expounded on the importance of information operations in the overall mix of military and non-military means of achieving political and strategic goals, where non-military means are becoming dominant.[69]

Russia's interference in Ukraine and its subsequent military operations in Crimea and the Donbass were popularly described as hybrid warfare. As the term became *en vouge*, the emphasis on information warfare emerged as a distinguishing feature in explaining (or reinterpreting) the meaning of hybrid operations.[70]

Conclusions

Syntehtising the above examples of strategic communication in the context of armed conflicts in the post-1990 period, it is concluded that strategic communication has become increasingly central to military practice over the past decades. This evolution shows a consistent pattern over time (from the early 1990s to the present day), across various theatres of operation (Iraq, Afghanistan, Ukraine) and through armed forces of highly different character, complexity and size (regular armed forces, insurgent groups, terrorist organisations).

Future directions

From a conceptual point of view, one direction of future research could constitute in further analysing military theories/classics of military science to clarify the meaning of key concepts in strategic communication. Another direction of research could concentrate on the relationship between strategic communication and contemporary military concepts

---

65 Mölder–Sazonov 2018: 316.
66 Mattsson 2016 cited in Wallenius–Nilsson 2019: 404.
67 Vandiver 2014 cited in Mejias–Vokuev 2017: 1027–1042.
68 Hammond-Errey 2019: 12.
69 Pynnöniemi–Jokela 2020: 831–832.
70 Wither 2016: 76.

which describe the changing nature of armed conflict, such as hybrid warfare, asymmetric warfare and fourth generation warfare.

From an empirical point of view, potential lines of inquiry could include studies into military history to explore the evolution of strategic communication in warfare as well as studies regarding the interplay between strategic communication, kinetic military operations and the attainment of political-military goals in modern warfare.

References

Adamson, William G. (1997): *The Effects of Real-Time News Coverage on Military Decision-Making* (Report No. AU/ACSC/0304/97-03). Montgomery, AL: Air Command and Staff College. Online: https://doi.org/10.21236/ADA388336

Ågren, Malin – Sataoen, Hogne (2022): Becoming a "Normal" and "Ordinary" Organization through Strategic Communication? Discursive Legitimation of the Swedish Armed Forces. *International Journal of Strategic Communication,* 16(1), 50–69. Online: https://doi.org/10.1080/1553118X.2021.2014500

Garfield, Andrew (2007): The U.S. Counter-propaganda Failure in Iraq. *Middle East Quarterly,* 14(4), 22–32. Online: www.meforum.org/1753/the-us-counter-propaganda-failure-in-iraq

Hallahan, Kirk – Holtzhausen, Derina – van Ruler, Betteke – Verčič, Dejan – Sriramesh, Krishnamurthy (2007): Defining Strategic Communication. *International Journal of Strategic Communication,* 1(1), 3–35. Online: https://doi.org/10.1080/15531180701285244

Hammond-Errey, M. (2019): Understanding and Assessing Information Influence and Foreign Interference. *Journal of Information Warfare,* 18(1), 1–22.

Holtzhausen, Derina – Zerfass, Ansgar eds. (2015): *The Routledge Handbook of Strategic Communication.* London – New York: Routledge. Online: https://doi.org/10.4324/9780203094440

Johnson, Thomas H. (2018): Amil Khan: *Taliban Narratives: The Use and Power of Stories in the Afghanistan Conflict.* London: Hurst, 2018. Book review. *International Affairs,* 94(4), 960–961. Online: https://doi.org/10.1093/ia/iiy101

Magen, Clila (2017): Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods. *International Journal of Strategic Communication,* 11(4), 269–285. Online: https://doi.org/10.1080/1553118X.2017.1334207

Mallet, Elizabeth E. (1997): Propaganda and Psychological Operations as Tools of Warfare during the Persian Gulf Conflict, 1990–91. *Cambridge Review of International Affairs,* 10(2), 280–297. Online: https://doi.org/10.1080/09557579708400151

Mattsson, Peter (2016): Warfare Without Armed Confrontation: Russian Psychological Methods Directed against Sweden. In Almqvist, Kurt – Hessérus, Mattias (eds.): *Finland and Sweden – Partners with a Mutual Interest?* Stockholm: Axess Publishing AB.

McMaster, H. R. (2008): On War: Lessons to be Learned. *Survival,* 50(1), 19–20. Online: https://doi.org/10.1080/00396330801899439

Mejias, Ulises A. – Vokuev, Nikolai E. (2017): Disinformation and the Media: The Case of Russia and Ukraine. *Media, Culture and Society,* 39(7), 1027–1042. Online: https://doi.org/10.1177/0163443716686672

Mölder, Holger – Sazonov, Vladimir (2018): Information Warfare as the Hobbesian Concept of Modern Times – The Principles, Techniques, and Tools of Russian Information Operations in the Donbass. *The Journal of Slavic Military Studies*, 31(3), 308–328. Online: https://doi.org/10.1080/13518046.2018.1487204

Németh, József Lajos (2013): A (stratégiai) kommunikáció és a háború kapcsolata napjaikban. *Hadtudomány*, 23(1–2.), 129–139.

Németh, József Lajos (2020): A stratégiai kommunikáció (hadi)technikai vonatkozásai I. rész. *Haditechnika*, 54(4), 13–16. Online: https://doi.org/10.23713/HT.54.4.04

Németh, József Lajos (2021a): *Stratégiai Kommunikáció.* Online: http://real.mtak.hu/130375/1/Strat%C3%A9giai%20kommunik%C3%A1ci%C3%B3.pdf

Németh, József Lajos (2021b): Stratégiai kommunikáció: fókuszban az állam és a haderő. *Hadtudományi Szemle*, 14(2), 115–132. Online: https://doi.org/10.32563/hsz.2021.2.9

Nothhaft, Howard – Page Werder, Kelly – Verčič, Dejan – Zerfass, Ansgar (2018a): Editors' Introduction. *International Journal of Strategic Communication*, 12(4), 329–332. Online: https://doi.org/10.1080/1553118X.2018.1493484

Nothhaft, Howard – Page Werder, Kelly – Verčič, Dejan – Zerfass, Ansgar (2018b): Strategic Communication: Reflections on an Elusive Concept. *International Journal of Strategic Communication*, 12(4), 352–366. Online: https://doi.org/10.1080/1553118X.2018.1492412

Nothhaft, Howard – Schölzel, Hagen (2015): (Re-)Reading Clausewitz: The Strategy Discourse and its Implications for Strategic Communication. In Holtzhausen, Derina – Zerfass, Ansgar (eds.): *The Routledge Handbook of Strategic Communication.* London – New York: Routledge. 18–33.

O'Connor, Amy – Shumate, Michelle (2018): A Multidimensional Network Approach to Strategic Communication. *International Journal of Strategic Communication*, 12(4), 399–416. Online: https://doi.org/10.1080/1553118X.2018.1452242

Page Werder, Kelly – Nothhaft, Howard – Verčič, Dejan – Zerfass, Ansgar (2018): Strategic Communication as an Emerging Interdisciplinary Paradigm. *International Journal of Strategic Communication*, 12(4), 333–351. Online: https://doi.org/10.1080/1553118X.2018.1494181

Patrick, Brian A. – Thrall, Trevor A. (2007): Beyond Hegemony: Classical Propaganda Theory and Presidential Communication Strategy After the Invasion of Iraq. *Mass Communication and Society*, 10(1), 95–118. Online: https://doi.org/10.1080/15205430709337006

Paul, Christopher (2011): *Strategic Communication: Origins, Concepts, and Current Debates.* Santa Barbara: Praeger.

Pratt, Cornelius B. – Azuka Omenugha, Kate (2014): "My God is Not Your God": Applying Relationship Management Theory to Managing Ethnoreligious Crises in Sub-Saharan Africa. *International Journal of Strategic Communication*, 8(2), 100–125. Online: https://doi.org/10.1080/1553118X.2014.882338

Pynnöniemi, Katri – Jokela, Minna (2020): Perceptions of Hybrid War in Russia: Means, Targets and Objectives Identified in the Russian Debate. *Cambridge Review of International Affairs*, 33(6), 828–845. Online: https://doi.org/10.1080/09557571.2020.1787949

Robinson, Piers (1999): The CNN Effect: Can the News Media Drive Foreign Policy? *Review of International Studies*, 25(2), 301–309. Online: https://doi.org/10.1017/S0260210599003010

Rothenberger, Liane (2017): A Terrorist Group's Strategic Communication – The Case of the Red Army Faction. *International Journal of Strategic Communication,* 11(4), 286–305. Online: https://doi.org/10.1080/1553118X.2017.1339191

Royo-Vela, Marcelo – McBee, Katherine A. (2020): Is *IS* Online Chatter Just Noise?: An Analysis of the Islamic State Strategic Communications. *International Journal of Strategic Communication,* 14(3), 179–202. Online: https://doi.org/10.1080/1553118X.2020.1770768

Seiffert-Brockmann, Jens (2018): Evolutionary Psychology: A Framework for Strategic Communication Research. *International Journal of Strategic Communication,* 12(4), 417–432. Online: https://doi.org/10.1080/1553118X.2018.1490291

Sweeney, Matthew M. – Perliger, Arie – Pedahzur, Ami (2020): Reconstructing the Theater of Terror. *Small Wars and Insurgencies,* 32(3), 469–489. Online: https://doi.org/10.1080/09592318.2020.1794176

Tabak, Lior – Avraham, Eli (2018): Country Image Repair Strategies During an Asymmetrical Conflict: An Analysis of the Gaza Conflict in 2014. *International Journal of Strategic Communication,* 12(3), 237–251. Online: https://doi.org/10.1080/1553118X.2018.1464009

Vandiver, John (2014): SACEUR: Allies Must Prepare for Russia 'Hybrid War'. *Stars and Stripes,* 04 September 2014. Online: www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464

Van Ruler, Betteke (2018): Communication Theory: An Underrated Pillar on Which Strategic Communication Rests. *International Journal of Strategic Communication,* 12(4), 367–381. Online: https://doi.org/10.1080/1553118X.2018.1452240

Vyklický, Vladimir – Divišová, Vendula (2021): Military Perspective on Strategic Communications as the "New Kid on the Block": Narrating the Czech Military Deployment in Afghanistan and the Baltic States. *International Journal of Strategic Communication,* 15(3), 231–252. Online: https://doi.org/10.1080/1553118X.2021.1906681

Wakefield, Robert I. – Plowman, Kenneth D. – Curry, Alex (2015): Institutionalization in Public Relations: Another Step in Examining its Place in Strategic Communication. In Holtzhausen, Derina – Zerfass, Ansgar (eds.): *The Routledge Handbook of Strategic Communication.* London – New York: Routledge. 353–369.

Wallenius, Claes – Nilsson, Sofia (2019): A Lack of Effect Studies and of Effects: The Use of Strategic Communication in the Military Domain. *International Journal of Strategic Communication,* 13(5), 404–417. Online: https://doi.org/10.1080/1553118X.2019.1630413

Wilbur, Douglas (2017): Propaganda's Place in Strategic Communication: The Case of ISIL's Dabiq Magazine. *International Journal of Strategic Communication,* 11(3), 209–223. Online: https://doi.org/10.1080/1553118X.2017.1317636

Winter, Charlie (2020): Redefining 'Propaganda': The Media Strategy of the Islamic State. *The RUSI Journal,* 165(1), 38–42. Online: https://doi.org/10.1080/03071847.2020.1734321

Wither, James K. (2016): Making Sense of Hybrid Warfare. *Connections,* 15(2), 73–87. Online: https://doi.org/10.11610/Connections.15.2.06

Zerfass, Ansgar – Verčič, Dejan – Nothhaft, Howard – Page Werder, Kelly (2018): Strategic Communication: Defining the Field and its Contribution to Research and Practice. International Journal of Strategic Communication, 12(4), 487–505. Online: https://doi.org/10.1080/1553118X.2018.1493485

AARMS Vol. 22, No. 1 (2023) 91–99.

10.32565/aarms.2023.1.7

Hypersonic Weapon Systems as an Indicator of Changes in Concepts and Theories

Attila TARJÁNI[1]

Since the hypersonic weapon system has gotten into service, the military strategists try to assess what changes the new capability will cause in the current theories and concepts. Even though there is much discredit around the effectiveness of the system, everyone agrees that it will shape and change the security environment. However, the first worries focused on the changes of current nuclear strategy, inherently the weapon will implicate other significant changes in the character of war. At the theory level, the capability of the system can override the current A2AD concepts, it can compel the adversary by bargain power and it can also put the current warfighting concepts at risk. Therefore, the analysis should focus on every segment of the current concepts and theories to predict how the system changes and shape military science.

Keywords: *hypersonic, coercion theory, warfighting concept, competition continuum*

Introduction

Regarding future conflicts, nobody can predict what it will look like, but Clausewitz's theory will remain: "War is the realm of uncertainty."[2] Within the uncertainty, all nations want to avoid the long and costly war; therefore, the modern military technology is always looking for two main factors to ensure the effectiveness in combat: speed and distance.

Speed has multiple importance; the first is the ability to overwhelm the opponent and exploit the success; this was the central idea of the Blitzkrieg, the "Shock and Awe",[3] and it will probably remain dominant in the Multi-Domain Operation concept.

The second is the speed of the mobilisation and deployment, and how quickly can a nation project be a military power for the designated area. The distance highlights the importance of how closely the military should allocate or manoeuvre the weapon systems to ensure providing the desired effects. When a weapon system is flying at 27 times the

[1] LtCol, e-mail: attilatarjani@gmail.com

[2] Clausewitz 1976: 101.

[3] Klare 2019.

speed of voice,[4] and relatively has no distance limitation, it will shape and affect the two main factors at the strategic and operational level.

Wake up call of hypersonic threat

When Russian Defence Minister Sergei Shoigu announced that the Avangard hypersonic weapon system is operational and entered its service on 27 December 2019,[5] it may be an indicator of a challenge of changes. Even though the Avangard entered the service, the effectiveness (accuracy, distance, active measures, etc.) of the system is still questionable. Maybe it is also part of the Russian military deception or 'maskirovka',[6] but the initial success of the system set up different considerations.

Some of the current journals and articles say that "it's an impressive technical achievement but solves a problem that doesn't actually exist".[7] The fundamental of this scepticism is focusing only on the nuclear applications of the weapon system, and ignores the fact what kind of advantages could bring to the table the conventional warhead capability.

The advanced hypersonic weapon system capability is a game-changer, and it provides a significant advantage to super, or major powers by challenging each other's coercion capability; and creating a critical vulnerability in the current warfighting concepts.

Hypersonic weapons are categorised as traveling faster than Mach 5, and currently include three major classes: ballistic missiles, boost-glide vehicles and cruise missiles.[8] The ballistic category remains the same as was for decades with some improvement. But the other two types are relatively new. Hypersonic boost-glide vehicles are launched by rockets and their flatter trajectory allows the vehicle to re-enter the upper atmosphere. At this point, it uses an aerodynamic lift to go glide as it slowly descends in altitude.[9] The cruise missile has a smaller platform; therefore, it can be launched from a ship or airplane, it does not leave the atmosphere, and because it must carry the fuel, the range is shorter than the boost-glide vehicle.[10]

The most advanced hypersonic weapon currently is the Russian Avangard the deployment of which goes back for 30 years of research.[11] In accordance with the Russian publications, the weapon hit a practice target 6,000 km away in a test launch at the Dombarovskiy missile base in the southern Ural Mountains.[12] The impressive capability performance is not coming only from the sharp manoeuvres, but it has active

4 Mizokami 2019.
5 Marcus 2019.
6 Maskirovka (маскировка [disguise]) Russian military deception, is a military doctrine developed from the start of the twentieth century. The doctrine covers a broad range of measures for military deception, from camouflage to denial and deception (https://en.wikipedia.org/wiki/Russian_military_deception).
7 Mizokami 2019.
8 Wilkening 2019.
9 Wilkening 2019.
10 Klare 2019.
11 Mizokami 2019.
12 Marcus 2019.

countermeasures during the flight and has the versatility to carry multiple warheads. The multiple warhead can include nuclear, which can carry two megatons, (comparing with Hiroshima that was 16 kilotons), and conventional warheads.[13]

Hypersonic effects on the spot: Nuclear or conventional?

Even though the current defence systems cannot deal with the hypersonic weapon threat, it is not the nuclear strategy that suffers the inherent challenges. The average nuclear missile defence systems are designed against rogue nations' (such as Iran or North Korea) or extreme violent organisations' single asset-nuclear strike not against Russia.[14] Russia has too many nuclear weapons to deploy a strike, therefore, the mutually assured destruction (MAD) remains the holdback concept. While the rogue nations do not have the hypersonic capability, the super, or major powers have time to develop new missile defence systems or other counter-measures.

However, the hypersonic weapon systems are not the only consideration of the unnecessary arms race, the United States and Russia agreed to extend for five years the New Strategic Arms Reduction Treaty (New START) on 3 February 2021. The focus of the agreement is still the nuclear capability, and to limit the number of warheads, missiles, bombers and launchers.[15] These kinds of acts can be acceptable as cooperation within the competition continuum to maintain the balance of strategic capabilities. Although the treaty only monitors and does neither limit the number of non-deployed launchers nor prohibit deploying conventional warheads on them. The strategic level consideration is that START can be applied to hypersonic weapon systems, if the conventional warhead application is not limited.

The conventional warhead application probably can bring more advantages and create changes in combat and theories. That is why there is interest in hypersonic weapons because they could be used for coercion assets or pre-emptive strikes to attack high value and high pay off targets and denial of the adversary's anti-access/area denial (A2AD) systems.[16]

The competition continuum requires a kind of balance within the capabilities to maintain the international relationships and avoid war. Therefore, the START agreement can restrict the unnecessary arms race on nuclear weapons, but it cannot hold back the further development of other strategic-level capabilities.

On the other hand, the sunk cost problem predicts the other application of the hypersonic weapon systems. The resource consumption of the development of hypersonic weapon systems is already high. The achieved successes probably are not game-changers in the current nuclear strategy concepts, but the temptation of the new capability of speed

[13] Marcus 2019.
[14] Mizokami 2019.
[15] Bugos 2022.
[16] Klare 2019.

and distance in conjunct of low circular error probable (CEP) would shape the doctrines and concept to provide raison d'être for them.

The multi-domain concept already divided the battle areas for different segments, and the deep fire area is relatively new in concept. This area is described as beyond the feasible range of the conventional manoeuvre forces, but the strategic effect is much desired to shape the follow-on phases of the operation.[17] Considering the capabilities of the hypersonic weapon systems within the A2AD environment, and the necessity of avoiding the sunk cost of the development, the solution of application is already at hand.

Hypersonic as challenger of theories and concepts

The first, that ultimately has already been challenged, is the coercion theory. In accordance with coercion theory, there are three different acts: deter (by the threat of punishment or by the threat of denial), compellence and brute force. As the enemy or adversary acts, the method of the reaction changes as well. The primary concept of deterrence is to avoid war, while compellence is the tool to enforce the enemy to stop the actual actions to avoid the escalation of conflict. The brute force is the ruthless solution, when the adversary is not cooperating and the conflict is inventible.[18]

Coercion − even if it is deterrence, compellence or brute force – in many cases requires deployment to ensure that the speed and the distance are suitable considerations. Denial as a most effective coercion[19] must be within the striking range of the air force to undermine an adversary's ability to attain military aims.

Airpower is a coercive tool of choice providing high precision effects on discrete targets, or in the role of denial, it can disrupt military supplies and destroy key military infrastructure. Doing so, airpower can provide coercion in four types: punishment, denial, risk and decapitation.[20] Most of the currently issued aircraft still possess distance limitations, therefore, the aircraft carrier gets them close enough to ensure the desired coercion effect, what is usually called 'gunboat diplomacy'.[21]

Moreover, to ensure the survivability of the air assets in complex A2AD environment, other supporting capabilities are required to cover or guard their actions. The cost of the hypersonic missile is unknown by the author, but the assumption is that it is not close to the price of modern aircraft. Therefore, the risk of the operation is not the same, because the loss of the equipment and the highly trained pilot is inherently included in the mission of the airstrike. While the application cost of the hypersonic weapon system is added at the moment of the launch, and the risk is limited to the measurement of effectiveness and the effects on the escalation of the conflict. Obviously, the aircraft can execute more missions, or is even able to strike multiple targets, while the hypersonic weapon system can target one critical object, the balance of risk and costs are still worth considering.

17 Perkins 2017.
18 Biddle 2020.
19 Biddle 2020.
20 Biddle 2020.
21 Ghosh 2001.

While the air force assets owned the capability and the capacity for being the coercive tool with some limitation, the hypersonic weapon systems are the pretenders in many segments. 'Gunboat diplomacy' as a coercion action has still one significant advantage, it is marginal. The theory in practice probably requires some real movement to ensure the commitment of the act of force if needed. However, the unseen threat does not mean that it can be ignored. Knowing the fact that the strike can come at any time, to any critical location and there is no defence capability to react, is another kind of bargaining power. Moreover, if someone tries to compel and we have the tool of the threat of denying, it is a counter-bargaining power too.

The distance and the speed are ensured even from the homeland to compel other state or actor or can be considered as extended A2AD capability as deterrence by threat of denial. Doing so, it is vital to locate the critical assets or strategic allocation. Finding a fleet or locating an Airport of Debarkation (APOD) or Seaport of Debarkation (SPOD) is not a challenge with the current intelligence, surveillance and reconnaissance (ISR) technology. The hypersonic weapon system with conventional warheads can strike these key targets or locations with extended range consideration in extremely improved speed when the current defence systems are not able to deal with it.

Probably the current hypersonic weapon systems do not have this level of accuracy today, but even the slim chance to pose this threat is already a game-changer. At the theory level, hypersonic weapons are the perfect coercion assets because they can deny strategic movements, and they can decapitate the ability to fight. However, the application of the weapon system in this strategic distance has an inherent risk that is described as 'warhead ambiguity'. The detection and the attack assessment is getting more complicated because a hypersonic boost-glide vehicle can manoeuvre hundreds of kilometres in cross-range during their glide phase, and the target remains uncertain.[22] The risk that the defending nation has no time to assess the target and the warhead type and assume the worst, it is launching a nuclear strike.[23] This risk assessment sounds logical, but what if the adversary sends a direct strategic message, that if the crisis is escalating, he will use hypersonic weapons with conventional warheads to degrade the strategic movement capability. Does it justify any nuclear strike knowing that mutually assured destruction is still a valid concept?

Of course, hypersonic weapon systems have different coercive effects or effectiveness on different states or actors. The near-peer competitors try to keep up the continuum developing the measures and counter-measures. But the capability balance is just one part of the problem, and the way how to use it most effectively is another part. If it does not get right, it will be "the Maginot Line of the 21st century"[24] as P. W. Singer described the same challenges for robotic systems.

The others who are not considered near-peer competitors, the weapon is the ultimate asset to suffer the consequences. While the effective counter-measures are not at hand,

[22] Wilkening 2019.
[23] Klare 2019.
[24] Singer 2010: 210.

the small nations and actors "can find [themselves] utterly defenseless"[25] as Clausewitz referred. Therefore, the coercion theory is not limited to distance and speed by the major powers to ensure they will hopefully just avoid a war.

Probably the strategic level application includes too high risks today; the operational level advantages are already challenging the current warfighting concepts. Overviewing the U.S. military boxer's stance, as a warfighting concept, it is described as the strength, agility and resilience required to fight and win against any potential adversary.[26] The critical vulnerability is coming from the dependence on reliable communication, high-speed data links, sophisticated weapon tracking radar and long-range strike capable systems. Targeting those systems is very difficult while they are moving. But they must stop for a short period to operate, and this provides a window of opportunity to destroy, but it also requires a weapon system in short-range or very high speed travel.[27] As an example, Russia already has an air-launched anti-ship missile, called Kinzhal, traveling speed is 10 Mach to range up to 1,200 miles,[28] and the Iskander Mobile missile transporter–erector launchers (TELs) can attack conventional targets up to 500 km.[29]

In the joint warfighting concept, the loss of critical assets predicts two kinds of challenges: quantitative incompetence and the undesirable asymmetric capability ratio. Most of the critical assets (as radars, TELs, ships, etc.) are costly tools, and even a superpower cannot afford to create a massive amount of reserve. Therefore, the supplement of the lost assets is creating a costly or unaffordable war. Moreover, the worst-case scenario is if the friendly joint force loses its critical assets, but the adversary does not. It creates an undesirable asymmetric capability ratio, where even the small tactical units remain unharmed; the operational-level support does not exist for them anymore, and they are vulnerable to the adversary long-range and cross-domain effects.

Of course, the challenge already has created many counter-measure visions and research and development (RAND) efforts. The Directed Energy Weapons (DEW) are capable of destroying targets within a limited line of sight, but it requires fast detecting and a precise targeting process. The high-powered microwaves can fry the processors, or at least may prevent the weapon from fusing, therefore, they are very promising as counter-measure against the threat.[30] Both development concepts have some critical vulnerability, even if it comes from the range, reaction time, or power support requirements. The advantage of the microwave is that it does not require precise targeting, because the invisible wave is wider, however, the same advantage could be a disadvantage too, if the target location is covered by the allocation of other friendly elements. Moreover, any single solution cannot answer for the complex challenge; the application of hypersonic weapon systems with other domains or weapon systems jointly can override the advanced defence capability.

---

25 Clausewitz 1976: 77.
26 Dunford 2017.
27 Wilkening 2019.
28 Klare 2019.
29 Army Technology 2017.
30 Venable–Abercrombie 2019.

Many weapons can be employed for offensive and defensive purposes, but hypersonic weapons are primarily offensive.[31] If any super or major power would like to maintain a competitive advantage, it requires a comprehensive effort. The development of the hypersonic weapon and countermeasures is not enough. It needs revising the current warfighting concepts. The advantages of modern technology affect two of the principles of Joint Operations: mass and simplicity. The mass revised means is the mass of effects in offense and countermeasures, and the simplicity will lose the significance because the future combat is probably inherently complex.

In order to answer these challenges, it is a fundamental approach to ask the right question. The current analysis of the hypersonic weapon systems is focusing on the assets per se, however, the good question probably is how the hypersonic weapon systems can challenge the current coercion theory and can change the current warfighting concepts as a part of a multi-domain cross effects tool? The theory is far from any concept at the moment, but it seems to be a fact that the capability of what the missiles can bring to the table cannot be ignored. If Clausewitz is still right, and the war is thus an act of force to compel our enemy to do our will,[32] the existence of a tool that can pose decapitation power theoretically, already can be considered the power of compellence with a different way of an act of force.

Conclusions

Winston Churchill's words "Generals are always prepared to fight the last war" are truer than ever, and the global arms race seems inevitable. While the battlespace and domain are expanding, and the purpose and the character of war is changing, the critical capabilities needed for deterrence or achieving strategic goals are persistently going through different evolution.

All states try to avoid becoming utterly defenceless and do everything to keep the right balance in the competition continuum by technical developments and doctrinal reviews. Nonetheless, the new START is a proper initiative to limit the nuclear arms race, but less to restrict other further races to compensate for the effects in the arms race that the hypersonic weapon systems already have initiated. The effects that the system can bring to the table should be compensated even in defence systems, or in other capabilities – even offensive – in other domains.

While the hypersonic weapon systems are on the spot, and different studies agreed that the nuclear strategy will not change dramatically, other segments of the arms race are already speeded up. On the one hand, other states do not want to fall behind the hypersonic technologies, therefore, they invest heavily to keep up the tempo. Moreover, there are other segments of the system that needs improvement such as current hypersonic weapon circular error probable reliability or increase the range or speed, and last but not least improve the usability of the system.

---

31 Klare 2019.

32 Clausewitz 1976: 75.

On the other hand, the necessity of the counter-measures against the hypersonic weapon systems is generating other critical investments that are creating another type of vicious cycle within the arms race. None of the counter-measures considers a single silver bullet, because the effectiveness of the hypersonic weapon systems depends on the creativity of the adversary. It can be combined with other strategic capability or simply other kinetic- or non-kinetic element that could make the damage so effective. While the counter-measures are developing to answer the hypersonic challenges, the ready-to-use products could provide unique capabilities that can be used for another purpose, therefore, the vicious arms race is regenerating itself.

As Russian General Chief of the General Staff Valery Gerasimov described: "Each war is a unique case, demanding the establishment of a particular logic and not the application of some template".[33] The future competition or conflict requires different methods of thinking in the matter of distance, the array of forces, integrated protection, intelligence, synchronised effects, expanded sustainment and cross-domain information. The advantage that the modern weapon systems bring to the table is inherently questioning the 'raison d'être' of the current warfighting concepts. Having a military power that cannot answer to these kinds of threats is already defenceless. Depending on what is the purpose of political objectives, the hypersonic weapon threat can set up a preferred condition to put the enemy in a situation that is more unpleasant than the sacrifice the call on him can make.[34]

References

Army Technology (2017): Iskander Tactical Ballistic Missile System. *Army Technology,* 06 April 2017. Online: www.army-technology.com/projects/iksander-system/

Biddle, Tami Davis (2020): Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review,* 3(2), 94–109. Online: https://doi.org/10.26153/tsw/8864

Bugos, Shannon (2022): New START at a Glance. *Arms Control Association,* April 2022. Online: www.armscontrol.org/factsheets/NewSTART

Clausewitz, Carl von (1976): *On War.* Princeton: Princeton University Press. Edited and translated by Michael Howard – Peter Paret. Online: https://doi.org/10.1515/9781400837403

Coalson, Robert (2014): Top Russian General Lays Bare Putin's Plan for Ukraine. *The Huffington Post,* 02 September 2014. Online: www.huffpost.com/entry/valery-gerasimov-putin-ukraine_b_5748480

Dunford, Joseph Jr. (2017): From the Chairman: Maintaining a Boxer's Stance. *Joint Force Quarterly,* 86(3), 2–3. Online: https://ndupress.ndu.edu/Publications/Article/1218381/from-the-chairman-maintaining-a-boxers-stance/

Ghosh, P. K. (2001): Revisiting Gunboat Diplomacy: An Instrument of Threat or Use of Limited Naval Force. *Strategic Analysis: A Monthly Journal of the IDSA,* 24(11), 2005–2017. Online: https://doi.org/10.1080/09700160108455335

[33] Coalson 2014.
[34] Clausewitz 1976: 77.

Klare, Michael T. (2019): An 'Arms Race in Speed': Hypersonic Weapons and the Changing Calculus of Battle. *Arms Control Today*, June 2019. Online: www.armscontrol.org/act/2019-06/features/arms-race-speed-hypersonic-weapons-changing-calculus-battle

Marcus, Jonathan (2019): Russia Deploys Avangard Hypersonic Missile System. *BBC News*, 27 December 2019. Online: www.bbc.com/news/world-europe-50927648

Mizokami, Kyle (2019): Russia's New Hypersonic Weapon Flies at Mach 27. *Popular Mechanics*, 30 December 2019. Online: www.popularmechanics.com/military/weapons/a30346798/russia-new-hypersonic-weapon-mach-27/

Perkins, David G. (2017): Multi-Domain Battle. Driving Change to Win in the Future. *Military Review*, July–August 2017. Online: www.armyupress.army.mil/journals/military-review/english-edition-archives/july-august-2017/perkins-multi-domain-battle/

Singer, P. W. (2010): *Wired for War. The Robotics Revolution and Conflict in the 21st Century.* New York: Penguin Books. Online: https://doi.org/10.5325/utopianstudies.21.2.0375

Venable, Heather – Abercrombie, Clarence (2019): Muting the Hype over Hypersonics: The Offense–Defense Balance in Historical Perspective. *War on the Rocks*, 28 May 2019. Online: https://warontherocks.com/2019/05/muting-the-hype-over-hypersonics-the-offense-defense-balance-in-historical-perspective/

Wilkening, Dean (2019): Hypersonic Weapons and Strategic Stability. *Survival*, 61(5), 129–148. Online: https://doi.org/10.1080/00396338.2019.1662125

AARMS Vol. 22, No. 1 (2023) 101–114.

10.32565/aarms.2023.1.8

Artificial Intelligence Landscape in South America

Anna URBANOVICS[1]

South American countries have also started to develop national AI strategies. The aim of the study is to provide a comparative analysis of strategy development processes in five South American countries: Argentina, Brazil, Chile, Colombia and Peru. For the quantitative analysis, I used data from the OECD AI Policy Observatory (Artificial Intelligence Policy Observatory) and other international databases, while for the qualitative analysis, I used document analysis on national strategies. The countries surveyed have taken different paths in preparing their national strategies, but the common point is that in all of them the strategy is part of a larger digitisation agenda. Although the AI strategies of the countries in the region are still at an early stage, the existence of national intent will allow progress in terms of both national and regional regulation, with the potential for these countries to become AI powers.

Keywords: *South America, artificial intelligence, strategic analysis, AI policy development*

Introduction

Artificial intelligence (AI) has not yet been given a single definition, as it is a very diverse umbrella term applied to a wide range of hybrid technologies used in many ways, both public and private. Artificial intelligence was first mentioned at a summer internship at Dartmouth University in 1956, and today there are around 70 different definitions.[2] According to one, "artificial intelligence is that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment".[3] The official OECD definition is: "An AI system is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations, or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g., with machine learning), or manually; and (iii) use model inference to

[1] University of Public Service, e-mail: urbanovics.anna@uni-nke.hu
[2] Cussins Newman 2019: 1–94.
[3] Nilsson 2010.

formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy."[4]

The 21st century is the age of artificial intelligence, and the international community associates the latest technological revolution with this technology. Applying AI can help a state achieve a more competitive and better performing national economy. This is why AI is now referred to as the latest "space race […] where world superpowers battle to define generations of technology to come".[5] While AI promises many benefits, it is also a timely reminder that states that lag behind in this race are missing out, due to inequalities in access to AI.[6] Competition is fierce, but the way forward is still uncertain as far as the use of AI is concerned.[7] Although the future of AI is still unpredictable, its greatest benefit, reduced costs, is already being felt by states. South American countries also try to catch up in the race for AI power, and in recent years seven countries have developed their own national strategies.[8]

The study compares the AI strategies and policies of five South American countries, Argentina, Brazil, Chile, Colombia and Peru, using a mixed methodology. The analysis aims to provide an overview of the current state of AI and the regulatory environment in these states. In Hungarian language, so far, no such topic has been published focusing on the region, although several topics (including cybersecurity and Latin American migration tendencies) have been covered by strategic document analysis.[9]

This introduction is followed by the core functions of artificial intelligence strategies in national AI policy and the research methodology. I will then present the results of the quantitative and qualitative analysis. Finally, the study concludes with conclusions and options for the way forward.

Core functions of AI strategies

Artificial intelligence can also be a stepping stone for developing regions to improve quality of life and break out of perpetual underdevelopment.[10] The use of technology can bring about significant changes in societies, national economies and public services.[11] Seizing the opportunity, South American countries have also joined the AI race, prioritising public capacity building, creating national strategies, training local talent, research and development, and the development of data infrastructure and an ethical framework for AI.[12] Tim Dutton[13] described this process as a race to become a global AI power. Andrés

4 OECD (2019.
5 Gershgorn 2018.
6 Miller–Stirling 2019.
7 Miller–Stirling 2019.
8 Montoya–Rivas 2019: 1–8.
9 Thomázy 2021: 58–74; Urbanovics–Guajardo Santana 2022: 89–104.
10 Sanchez-Pi et al. 2021.
11 Veronese – Nunes Lopes Espiñeira Lemos 2021: 1–31.
12 TMG 2020.
13 Dutton 2018.

Ortega[14] defined this strategy-making process as the geopolitics of the fourth industrial revolution.

In mapping AI strategies, UNESCO experts described the recent period as the "flood of AI strategies".[15] The field of AI raises a number of regulatory issues, including a number of regional, national and cross-border regulations. In addition to the opportunities already created by the exponential growth of transnational Internet litigations, the sharing of jurisdictional areas and international cooperation in Big Data structures, the race to find automated and computational mechanisms in the fields of inventions, applications and artificial intelligence are creating a convergence of interests and coordinated cooperation of public and non-public actors in the fields of the interfaces between law and technology.[16] However, it is worth pointing out that each state develops its national AI strategy according to its own experience and values, and thus there are significant differences and shifts in emphasis among them.[17] In general, the criteria are the following:[18]

- the role of scientific research in the field of AI
- professional development, preparing the labour market for the use of AI
- public capacity development and the development of educational institutions
- public–private cooperation in the field of AI
- standards, regulations and the development of data and digital infrastructure

Due to the different emphases, strategies can also differ greatly in their level of maturity.

In the South American region, Argentina, Colombia and Uruguay are among the countries recognised by the OECD as active in the field of AI. Although many initiatives are underway in the region to coordinate national strategies, these have not yet been achieved.[19] One such international initiative is the movement launched by the United Nations Economic Commission for South America and the Caribbean (ECLAC). ECLAC seeks to make the states of the region leading AI powers and to embed national policies in a global context. In the current phase of its integration efforts, ECLAC seeks to achieve "open regionalism" between states, along the lines of the EU, a phase aimed at technological integration. Two related reports have been published entitled *Industrial and Technological Policies in South America*[20] and *Human Resources for the Digital Transition in South America*.[21] In this sense, AI has become a policy that has an impact on both the economy and social processes, with which ECLAC is coordinated to achieve a "digital regional market" (digital common market).

Another example concerns the use of AI in specific tasks, such as the fight against corruption, as illustrated by the Organization of American States (OAS) initiative.[22] OAS supports "e-Government Leaders for South America and the Caribbean" (RedGEALC),

14 Ortega 2019: 21–24.
15 Dutton 2018.
16 Polido 2019.
17 Polido 2020: 229–256.
18 Dutton 2018.
19 Veronese – Nunes Lopes Espiñeira Lemos 2021: 1–31.
20 CEPAL 2017.
21 Katz 2018.
22 Moss 2019.

a network that relies entirely on AI.[23] Since 2003, the network has brought together the authorities of the digital government organisations of the LAC region. Its composition makes it a unique instrument to promote horizontal cooperation, the development of participatory policies on digital government, the training of public officials, and the exchange of solutions and experts among the countries of the region. The network enables member countries to share essential knowledge about the development of national digital government strategies. Its general objective is to support digital government policies that put the citizen at the centre, especially in relation to the most vulnerable populations.[24] In addition, there are some non-governmental initiatives, such as IA Latam, a network of businesses and researchers.[25] Even the Inter-American Development Bank (IADB) has endorsed the Fair LAC report, which comprehensively covers the policies of the twelve countries of the region.[26]

Methodology

The present analysis is based on a mixed methodology, with regional comparisons using quantitative and qualitative tools providing the main results. According to Bolgov,[27] the effectiveness of a country's policy objectives and strategies can be measured by global indices and rankings, but it is important to emphasise that these rankings may give a different picture of the situation of individual states, due to their different methodologies. In addition to the general indicators presented in the introduction, the analysis relies on open databases available on the Internet, focusing on the most recent data.

One of the core elements is the Government AI Readiness Index,[28] which basically measures the readiness of public organisations to use AI technology in 160 countries in 10 dimensions and across 42 indicators. The analysis is prepared and published annually by Oxford Insights. This index is important due to the fact that it presents the national preparedness to use AI technology from the aspect of the national policy.

Other complex indices also contribute to the report, including the Global Innovation Index,[29] published annually by the World Intellectual Property Organization (WIPO), which measures the innovation potential of 132 economies across 81 indicators.

The IMD World Digital Competitiveness Index[30] measures countries' digital readiness along three pillars: knowledge, technology and future readiness. The 2021 report shows that the higher scores the country reaches in terms of future readiness, the more quickly it adapts to a changing technological environment, and the more competitive it is.

---

23 RedGEALC (www.redgealc.org/).
24 RedGEALC.
25 IA Latam (https://ia-latam.com).
26 Gómez Mont et al. 2020.
27 Bolgov 2020: 259–263.
28 Government AI Readiness Index 2021.
29 Global Innovation Index 2021.
30 IMD World Digital Competitiveness Index 2022.

Government technology maturity is measured and compared using the GovTech Maturity Index,[31] which is based on 46 indicators in 4 dimensions in 198 countries, as measured by the World Bank. The dimensions are the following:

1. Basic Governance Systems Index
2. Provision of Public Services Index
3. Citizen Involvement Index
4. GovTech Incentive Index

For qualitative analysis, we use the AI Policy Observatory platform[32] of the Organisation for Economic Co-operation and Development (OECD). It is a platform that gathers and monitors the development of national policies on AI, with voluntary participation from Member States, with the aim of enabling states to develop their regulatory framework in a coordinated way at international level.

In May 2019, OECD member countries established the AI principles along which they are actively developing their policies. These are the following:

1. inclusive growth and sustainability
2. human-centred values and fairness
3. transparency and explainability
4. stability and security
5. accountability
6. investing in AI R&D
7. fostering a digital ecosystem for AI
8. providing an enabling policy environment for AI
9. building human capacity
10. international cooperation for AI

The countries involved in the comparative analysis are member states of the OECD AI initiative. Qualitative document analysis was carried out along the following national-level strategies:

- Argentina: Artificial Intelligence National Plan (2019)[33]
- Brazil: Brazilian Artificial Intelligence Strategy (2021)[34]
- Chile: Artificial Intelligence National Policy (2019)[35]
- Colombia: Artificial Intelligence National Strategy (2019)[36]
- Peru: National Artificial Intelligence Strategy (2021)[37]

It is worth noting here that in Chile and Argentina, regulation at the national level is not referred to as a strategy.

---

31 GovTech Maturity Index 2021.
32 OECD AI Policy Observatory 2022.
33 Plan Nacional de Inteligencia Artificial Argentina 2019.
34 Estratégia Brasileira de Inteligência Artificial Brazil 2021.
35 Política Nacional de Inteligencia Artificial Chile 2019.
36 Estrategia Nacional de Inteligencia Artificial Colombia 2019.
37 Estrategia Nacional de Inteligencia Artificial Peru 2021.

South American digital readiness

To analyse and contextualise national AI strategies, it is also worth reviewing some indicators related to the digital readiness of the countries surveyed.

The IMD World Digital Competitiveness Index 2021 ranks Chile 39th, Brazil 51st, Peru 57th, Colombia 59th and Argentina 61st. If we look at the pillars that make up the ranking, we see that in most countries the technology pillar is advanced, while in Chile and Peru the digital knowledge and competences pillar stands out.

In terms of innovation potential, the latest data show that Chile stands out (53rd in 2021), followed by Brazil (57th) and Colombia (67th). However, in recent years (2017–2021), Argentina and Brazil have moved up, while Chile and Colombia have moved down and Peru has maintained its 70th position.[38] According to the WIPO report, Peru is a global leader in the indicator "Availability of loans from microfinance institutions", stands at 18th place at "Graduates in science and engineering" and 22nd place at "Utility models".[39]

The artificial intelligence market is forecast to grow strongly in the region.

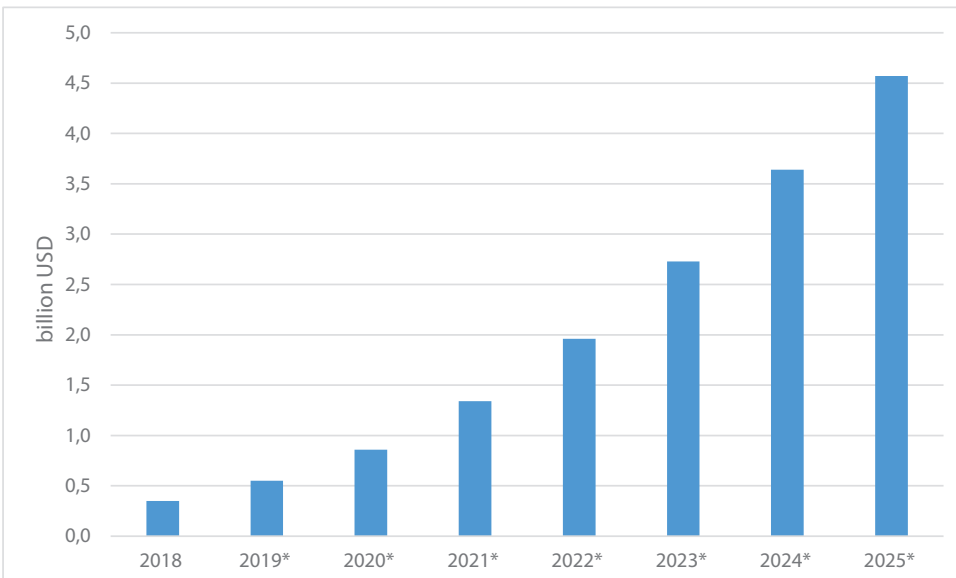

Figure 1: Projected revenues of the South American artificial intelligence market 2018–2025

Source: Compiled by the author based on the data of Statista 2019a.

According to Statista (2019a), the South American region could reach $4.57 billion in revenue by 2025. In 2021, however, the region's artificial intelligence market reached

[38] Global Innovation Index 2021.
[39] Global Innovation Index 2021.

$1.34 billion in revenue, with a number of emerging technology companies and organisations, including the machine learning and natural language recognition sectors.

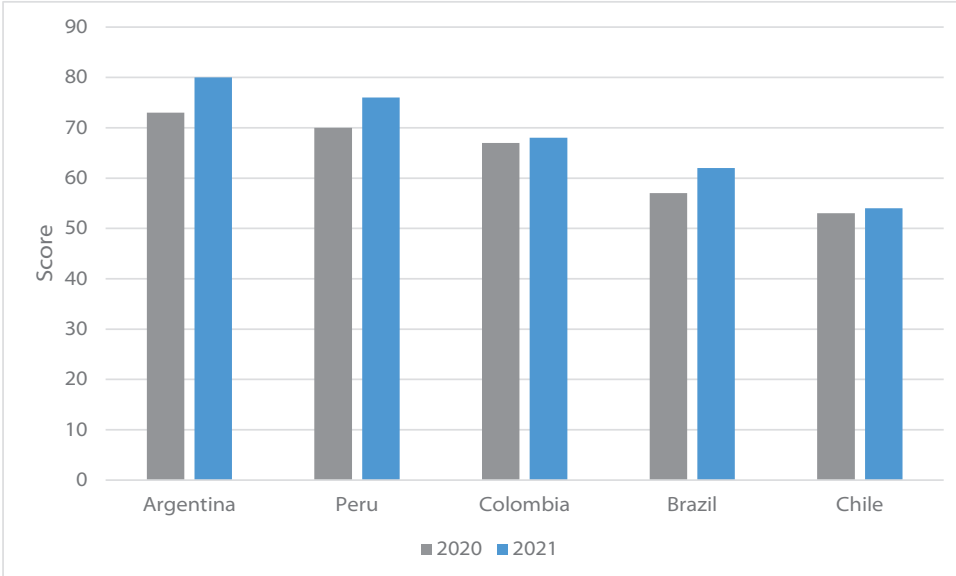

Figure 2: GovTech maturity scores for the surveyed states in 2020 and 2021

Source: Compiled by the author based on the data of GovTech Maturity Index 2021.

In the context of public readiness for AI, it is also worth studying the GovTech maturity index, where the overall scores show that Argentina, Peru and Colombia stand out. Of the three pillars that make up the index, Argentina, Brazil and Peru scored the highest in the government pillar, while Colombia and Chile scored the highest in the data and infrastructure pillar. Brazil stands out in the governance pillar, and Colombia in both the technology, and data and infrastructure pillars.

In 2019, a survey on the public use of AI in the public sector was conducted. In both Brazil and Chile, 15% of the respondents said that the state should not use these technologies, while Brazil has the highest proportion (29%) of those who think that the government should be allowed to use these technologies without restrictions as long as the situation requires. The questionnaire asked about the use of artificial intelligence and facial recognition in the context of maintaining law and order. The exact results are summarised in Figure 3.

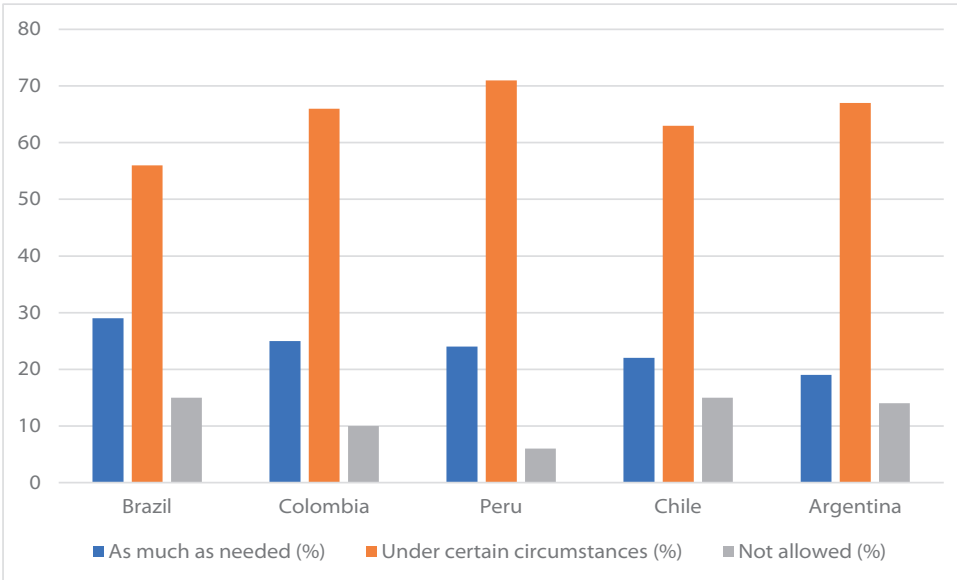

Figure 3: Results of the public opinion survey for the surveyed states on the adoption of AI and facial recognition by the state to maintain law and order

Source: Compiled by the author based on the data of Statista 2019b.

Comparison of national AI strategies in the countries surveyed

Although it is beyond the scope of the present study to analyse the AI strategies of the countries under study in detail, we can compare them along content elements, both in terms of strategy and implementation.

One such aspect is the definition of the exact time frame, which is as follows: Argentina (2019–2029, 10-year framework), Chile (2021–2030, 9-year framework), Colombia (2019–2022, 3-year framework), Peru (2021–2026, 5-year framework). Brazil does not have an exact time frame. Setting out time frame is crucial in terms of implementing the strategies as it puts pressure on the state to achieve strategic goals within a certain period. Another aspect is the coordinating organisation, in most cases the ministries of science and technology. This is different in Colombia, where the Ministry of Information and Technology, the Ministry of Education, the Ministry of Science, Technology and Innovation, the Office of the Department of President of Colombia, the National Planning, and in Peru, where the responsible bodies are the Office of Government and Digital Transformation, the Office of the Council of Ministers.

When the strategies of South American countries are examined collectively, several key themes and objectives emerge. For example, they often seek to catalyse economic development through funding and incentives for research and development, transform the labour market and strengthen talent pools through refresher programs, and promote

strong governance and data sharing, including the opening of public administration data. It should be noted that all strategies include provisions to ensure that AI systems are designed and implemented in an ethical and trustworthy manner (for example, through the creation of ethics-related frameworks and governance bodies). In addition, several strategies emphasise international collaboration, particularly those from Argentina, Brazil, Chile and Peru. Some of them include more specialised components, such as the gender perspective that Chile incorporates in AI research and development. Looking at the targets set, we can see that Argentina, Brazil and Colombia have the most complex strategies. The most common targets are:

- achieving inclusive and sustainable economic growth through AI (Argentina, Chile, Colombia, Peru)
- research and development, education and innovation using AI (Argentina, Brazil, Chile, Colombia)
- establish an ethical and cybersecurity framework for AI (Brazil, Chile, Colombia)
- reducing social inequalities through the use of artificial intelligence (Colombia, Peru)
- becoming a regional AI "powerhouse" in South America (Argentina, Peru)

But if we look at quantified targets, which by their very nature are well measured in terms of effectiveness, we find none in Brazil or Peru. The national strategies of these two countries set objectives in general terms and do not link them to a set of measurable indicators. The only exception to the Brazilian strategy is the requirement for at least 12 state governments to adapt AI to their workflows by 2022. Argentina and Chile have action plans to ensure measurability, while in the Colombian strategy, the objectives are well measurable in terms of their formulation. The policy areas most frequently concerned are government (in all the countries surveyed), industry and business (Argentina, Brazil, Colombia, Peru), and education (Brazil, Chile, Colombia, Peru). However, defence policy is only reflected in the Brazilian strategy. It is important to note that by the Research, Development, Test and Evaluation (RDT&E) agreement made in April 2022 between Brazil and the United States, the two nations strengthened the cooperation and defence technology exchange. Three Brazilian cutting-edge defence technology projects have caught the attention of the U.S. military, including mind mapping, bioprinting and artificial intelligence.[40]

It is also worth looking at the OECD principles in terms of how much and what principles are taken into account in the strategy.

Based on this, Argentina shows the most complex picture, having incorporated all 10 OECD AI principles into its strategy, followed by Peru with 9. In Chile, however, only three have received attention: developing the digital ecosystem for AI, providing an enabling policy environment for AI and building human capacity.

Social inequality and job insecurity are the most frequently cited *societal challenges* related to AI identified in the strategies in the countries surveyed. In addition, environmental sustainability and climate change, as well as the impact of the technological revolution are also identified as potential risk factors.

[40] Barretto 2022.

Table 1: Analysis of AI strategies of the surveyed countries based on OECD principles

OECD principles	Argentina	Brazil	Chile	Colombia	Peru
Inclusive growth and sustainability	X			X	X
Human-centred values and fairness	X	X			X
Transparency	X	X			X
Stability and security	X				
Accountability	X				X
Investing in AI R&D	X	X			X
Digital ecosystem for AI	X	X	X	X	X
Providing an enabling policy environment for AI	X	X	X	X	X
Building human capacity	X	X	X	X	X
International cooperation for AI	X	X			X

Source: Compiled by the author based on the data of the OECD AI Policy Observatory 2022.

Furthermore, it is necessary to address the *regulatory environment* and the background to the national AI strategy in the countries studied. The data show that in all cases the AI strategy was part of a larger public programme for digital development. The importance of artificial intelligence was discussed by Brazil and Colombia along efforts related to digital transformation of the public sector, by Peru along the public sector as a strategic priority, and by Chile along the importance of AI in education and R&D. In Argentina, the AI strategy is part of Argentina's 2030 Digital Agenda and one of the 2030 national challenges of the Innovative Argentina Strategy. On the last day of President Mauricio Macri's mandate (December 2015 – December 2019), the government released the AI National Plan. The document was the end result of a drafting process that lasted more than a year and consultations with different actors in thematic panels and meetings. One of its main objectives is to build capacity so that Argentina assumes a leading role in technology in order to boost local development, instead of being a simple consumer of foreign technologies and advancements. Furthermore, the plan lays the foundation for the new government as a guideline, mentioning priorities including the talent, data, supercomputer infrastructure, research, development and innovation, implementation in the public and private sectors, impact on employment, ethics and regulation, international involvement and innovation laboratories. In Brazil, in recent years, measures have been defined along the lines of the strategy called the E-Digital strategy (Brazilian Digital Transformation Strategy) and the General Data Protection Law. The current AI strategy is the result of a two-year consultation with more than a thousand participants, the first to focus on AI at the federal level. In May 2019, the federal government, together with the Brazilian Competitiveness Movement, organised the AI Seminar on Digital Transformation with the participation of relevant authorities, scholars and systems developers. As the result of their work, the national AI strategy has been launched. The strategy has two types of axes: vertical (research, development, innovation and entrepreneurship; implementation in the public sector; implementation in the productive sectors; and public security); and

cross-cutting (legislation, regulation and ethical aspects; use; and international and AI governance). Besides these, the government established specific working groups focusing on areas of health, agriculture, industry and intelligent cities. In Chile, the publication of the AI strategy was planned for April 2020, but the Covid-19 epidemic and the series of protests that started in the autumn of 2019 delayed the work (see Pólyi–Thomázy[41] on the reasons for the protests in 2019), so it was not published until early 2021. The longer period allowed for the organisation of a strategy-making process based on an even broader consultation. The strategy focuses mainly on the use of AI by Chileans, involving them in the creation of legal, ethical, social and economic regulations. In November 2019, Colombia adopted a digital transformation, including an AI strategy. The policy seeks to create international alliances for the innovation, design and implementation of initiatives that foster entrepreneurship and digital transformation. Its priorities are to create an AI market in the country and attract global talent. In Peru in 2018, Decree 1412 and the Law on Digital Governance lay the foundations for the AI strategy.

Conclusions and options

Artificial intelligence is one of today's key strategic technologies, present in many areas of the economy and society. Developing countries are expecting technology to rise above others in terms of economic growth and boost their competitiveness, while the great powers are in increasing competition for the power of artificial intelligence. Several regional and international initiatives seek to harmonise and control the use of AI and encourage states to cooperate. One such initiative is the OECD AI Policy Observatory, which monitors developments in countries on an ongoing basis. Several South American countries have joined this competition and the development of national strategies is inevitable for the responsible use of AI, of which this study comparatively examines the strategies and developments in Argentina, Brazil, Chile, Colombia and Peru. Some results are worth highlighting, which illustrate the current situation and the way forward.

On the one hand, South American countries are committed to digital switchover and have been modernising both the private and public sectors accordingly. They have already prepared their AI strategy to be competitive, but in terms of cybersecurity (data protection, critical infrastructure protection), they are more in the mid-range, among the developing regions. But their e-government developments classify them among the prepared states. Many international and regional initiatives are trying to harmonise their AI strategies, but this has not yet been achieved, so strategies are formulated at national level.

In the context of the strategy analysis, it is worth noting that although all the countries studied have an AI strategy, the precision of the strategies varies. This is illustrated both by the lack of measurable targets in some cases and by the fact that only Argentina's and Colombia's strategies seek to take into account as many AI principles as possible. When analysing the regulatory context of these strategies, it is clear that they are the result of

[41] Pólyi–Thomázy 2019: 79–103.

the digitisation of the state, which both demonstrates the strategic importance of AI and highlights the potential for a much larger, robust programme.

Although the Covid-19 epidemic has in many cases caused a setback in the strategy-making process, the key objective for the states in the region is to reduce social inequalities through the use of AI. National regulations can be a good starting point, but the real breakthrough could come from regional integration efforts, mainly based on the EU model, the creation of a so-called "digital regional market".

References

Barretto, Andréa (2022): Brazil and the United States to Develop Joint Defense Technology. *Diálogo*, 17 August 2022. Online: https://dialogo-americas.com/articles/brazil-and-the-united-states-to-develop-joint-defense-technology/#.Y-ZZonbMK5c

Bolgov, Rodomir (2020): *The UN and Cybersecurity Policy of Latin American Countries.* 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG). 259–263. Online: https://doi.org/10.1109/ICEDEG48599.2020.9096798

CEPAL (2017): *Políticas Industriales y Tecnológicas en América Sur.* Santiago: CEPAL, November 2017. Online: www.cepal.org/es/publicaciones/42363-politicas-industriales-tecnologicas-america-latina

Cussins Newman, Jessica (2019): Toward AI Security. Global Aspirations for a More Resilient Future. *CLTC White Paper Series*, February 2019, 1–94. Online: https://cltc.berkeley.edu/wp-content/uploads/2019/02/Toward_AI_Security.pdf

Dutton, Tim (2018): An Overview of National AI Strategies. *Politics + AI*, 28 June 2018. Online: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

Estratégia Brasileira de Inteligência Artificial Brazil (2021). Online: www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria_mcti_4-979_2021_anexo1.pdf

Estrategia Nacional de Inteligencia Artificial Colombia (2019). Online: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf

Estrategia Nacional de Inteligencia Artificial Peru (2021). Online: https://cdn.www.gob.pe/uploads/document/file/1909267/National%20Strategy%20for%20Artificial%20Intelligence.pdf

Gershgorn, Dave (2018): AI Is the New Space Race: Here's What the Biggest Countries Are Doing. *Quartz*, 02 May 2018. Online: https://qz.com/1264673/ai-is-the-new-space-race-heres-what-the-biggest-countries-are-doing

Global Innovation Index (2021). Online: https://doi.org/10.34667/tind.46596

Gómez Mont, Constanza – Del Pozo, Claudia May – Martínez Pinto, Cristina – Martín del Campo Alcocer, Ana Victoria (2020): *Artificial Intelligence for Social Good in South America and the Caribbean. The Regional Landscape and 12 Country Snapshots.* Washington, D.C.: IADB. Online: https://doi.org/10.18235/0002393

Government AI Readiness Index (2021). Online: https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/61ead0752e7529590e98d35f/1642778757117/Government_AI_Readiness_21.pdf

GovTech Maturity Index (2021). Online: https://openknowledge.worldbank.org/handle/10986/36233

IMD World Digital Competitiveness Index (2022). Online: www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

Katz, Raúl (2018): *Capital Humano para la Transformación Digital en América Latina.* Comisión Económica para América Latina y el Caribe. Online: www.cepal.org/es/publicaciones/43529-capital-humano-la-transformacion-digital-america-latina

Miller, Hanna – Stirling, Richard (2019): *Government Artificial Intelligence. Readiness Index 2019.* Oxford Insights. Online: https://ec.europa.eu/futurium/en/system/files/ged/ai_readiness_index_2019__0.pdf

Montoya, Laura – Rivas, Pablo (2019): *Government AI Readiness Meta-Analysis for Latin America and the Caribbean.* 2019 IEEE International Symposium on Technology and Society (ISTAS), Medford, MA, USA, 15–16 November 2019. 1–8. Online: https://doi.org/10.1109/ISTAS48451.2019.8937869

Moss, Loren: Organization of American States Redoubles Efforts to Combat Corruption with Big Data, Artificial Intelligence & Analytics. *Finance Colombia,* 13 August 2019. Online: www.financecolombia.com/organization-of-american-states-redoubles-efforts-to-combat-corruption-with-big-data-artificial-intelligence-analytics/

Nilsson, Nils J. (2010): *The Quest for Artificial Intelligence. A History of Ideas and Achievements.* Cambridge: Cambridge University Press.

OECD AI Policy Observatory (2022). Online: https://oecd.ai/en/

OECD (2019): *Artificial Intelligence in Society.* Online: https://doi.org/10.1787/eedfee77-en

Ortega, Andrés (2019): Geopolítica de la Cuarta Revolución Industrial. *Economistas,* (165), 21–24. Online: www.cemad.es/wp-content/uploads/2019/10/Geopolitica-4RI.pdf

Plan Nacional de Inteligencia Artificial Argentina (2019). Online: https://ia-latam.com/wp-content/uploads/2020/09/Plan-Nacional-de-Inteligencia-Artificial.pdf

Polido, Fabrício Bertini Pasquot (2019): *Direito Internacional Privado nas Fronteiras do Trabalho e da Tecnologias: ensaios e narrativas na era digital.* Rio de Janeiro: Lumen Iuris.

Polido, Fabrício Bertini Pasquot (2020): Inteligência artificial entre estratégias nacionais e a corrida regulatória global: rotas analíticas para uma releitura internacionalista e comparada. *Revista da Faculdade de Direito UFMG,* (76), 229–256. Online: https://doi.org/10.12818/P.0304-2340.2020v76p229

Política Nacional de Inteligencia Artificial Chile (2019). Online: www.minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf

Pólyi, Csaba – Thomázy, Gabriella (2019): A chilei tüntetések hátterében álló tényezők. *Nemzet és Biztonság,* 12(3), 79–103. Online: https://doi.org/10.32576/nb.2019.3.8

Sanchez-Pi, Nayat – Martí, Luis – Bicharra Garcia, Ana Cristina – Baeza Yates, Ricardo – Vellasco, Marley et al. (2021): *A Roadmap for AI in South America. Side event*

AI in South America of the Global Partnership for AI (GPAI). Paris: Paris Summit, GPAI Paris Center of Expertise.

Statista (2019a): *Revenues from the artificial intelligence (AI) software market in South America from 2018 to 2025 (in billion U.S. dollars)*. Online: www.statista.com/statistics/721751/latin-america-artificial-intelligence-market/

Statista (2019b): *Public opinion on the governmental use of artificial intelligence (AI) and facial recognition in selected countries in South America in 2019*. Online: www.statista.com/statistics/1101603/government-use-ai-latin-america/

Thomázy, Gabriella (2021): Migrációs stratégiák: Dél-Amerika vs. Európa. Ecuador, Kolumbia, Magyarország és Spanyolország összehasonlító elemzése. *Hadtudomány*, 31(2), 58–74. Online: https://doi.org/10.17047/HADTUD.2021.31.2.58

TMG (2020): Overview of AI Policies and Developments in South America. *TMG Report*, February 2020. Online: www.tmgtelecom.com/wp-content/uploads/2020/03/TMG-Report-on-Overview-of-AI-Policies-and-Developments-in-Latin-America.pdf

Urbanovics, Anna – Guajardo Santana, Rodrigo (2022): Estrategias de ciberseguridad en los países latinoamericanos – un análisis comparativo. *Acta Hispanica*, (4). 89–104. Online: https://doi.org/10.14232/actahisp.2022.0.89-104

Veronese, Alexandre – Nunes Lopes Espiñeira Lemos, Amanda (2021): Trayectoria normativa de la inteligencia artificial en los países de Latinoamérica con un marco jurídico para la protección de datos: límites y posibilidades de las políticas integradoras. R*evista Latinoamericana de Economía y Sociedad Digital*, (2), 1–31. Online: https://doi.org/10.53857/MZBU2371

AARMS Vol. 22, No. 1 (2023) 115–132.

10.32565/aarms.2023.1.9

What Can Privacy Mean in Data-Driven Societies?

The Security Policy Contexts of the Data Management Culture in the People's Republic of China and the European Union[1]

Tünde LENDVAI,[2] András TÓTH[3]

The purpose of this article is to present the basis for building trust within the European Union, through which the authors illustrate the importance of the protection of personal data as a fundamental requirement in both the EU and its Member States' legal environments. In addition, the authors have examined the Chinese Social Credit System, which by its design and operation is not primarily focused on building trust and is therefore not the most appropriate solution for building trust. The authors conducted a SWOT analysis comparing the EU and Chinese principles to achieve their objectives. They also conducted interviews with people who have personal experience with the Chinese credit point system. Based on the results obtained, they sought to justify their basic hypothesis that this type of credit system could not be applied within the EU.

Keywords: *Chinese Social Credit System, data-driven society, personal data, privacy, trust*

The People's Republic of China (hereinafter referred to as China) operates a unique data-based public administration system, the Social Credit System (in Mandarin: 社会信用体系, pinjin transliteration: shehui xinyong tixi). On the other hand, the European Union prioritises protecting the public's personal data, an obstacle to any Member State's efforts in this direction. Therefore, the basic regulation is the General Data Protection Regulation (GDPR), which aims to prevent the collection and processing of data about the public without their consent. Accordingly, it regulates how data is collected, processed, stored, erased, used and transferred.

The study uses a deductive approach and a qualitative assessment of secondary data to show how political and cultural traditions, as well as geopolitical and economic conditions have led to the development of a data management culture in China that is so different from

[1] The work was implemented in the framework of project TKP2020-NKA-09 funded by the National Research Development and Innovation Fund under the Thematic Excellence Program 2020.

[2] Junior IT Security Auditor, Black Cell Magyarország Ltd., e-mail: lendvaitunde96@gmail.com

[3] Associate Professor, University of Public Service, Signal Department, e-mail: toth.hir.andras@uni-nke.hu

European traditions and on which the social credit point system could be built. The Beijing leadership's operation of an extensive data collection and data-driven administrative approach both helps and hinders the state's security policy and cybersecurity efforts by applying a defence framework built around cyber warfare logic. To prove this thesis, the study explores the correlations between how the government's data disclosure requirement limits the ability of the major players in the Chinese IT market (Alibaba Group, Tencent, Baidu) to address cybersecurity vulnerabilities, which in turn reduces trust in Chinese IT services and the overall security of cyberspace. Within the European Union, the authors have reviewed the principles and practices that aim to build the trust that will help people use the systems and services available under the Digital Europe Programme without fear of their personal data being accessed by service providers and the public and non-public actors. To increase the validity of the results, the authors conducted expert interviews as part of primary data collection (see section *Interviews*). These focused on confidentiality, which is central to their research, and concerning which they formulated their basic research question about what confidentiality might mean in data-driven societies. In their analysis of the interviews, they examined what trends emerged in response to the questions related to each hypothesis, from which they could draw relevant scientific conclusions. The hypothesis were the followings:

- The European Union is making great efforts to build trust, but this can be threatened by technological, technical, or sociological influences from outside the Union.
- The Chinese Social Credit System is not based on trust, the reason being that the focus of data protection is on the state perspective and not on individuals, and therefore it is not feasible to implement this type of system in the EU.

The main objective of the research is to conduct a comparative case study of social credit scoring and data cultures controlled by the EU legal framework to prove, by answering the hypotheses, that introducing a credit scoring system is not feasible in a trust-based society. Furthermore, by comparing the two contexts, we can gain a better understanding of the social and legal implications of introducing credit scoring systems in EU countries.

Trust and privacy in the European Union

Many EU reports and strategies state that Europe is built on trust. Trust is essential because it is the basis for well-functioning relationships and is a key element in a system of properly operating democracies. Accordingly, leaders must do everything in the EU and its Member States to ensure that the necessary trust is built and sustained among citizens, businesses and organisations. In the digitalisation of Europe, information security, which is closely linked to trust, should be a key focus of attention at both public and executive levels. Therefore, Europe needs to act in a unified way in all areas of information security to ensure compliance within the Union and at the national level to build the necessary trust. To achieve this, the activities of governments and industry must not stop at EU

borders, and cooperation at the global level is essential to ensure adequate security and to maintain the trust that has been built up.[4]

All these considerations indicate that, in addition to efficiency and effectiveness, building legitimacy and trust is an important factor that governments need to consider in their innovation activities for digitisation. Therefore, when we talk about digitalisation, it is important to talk about the ethical use of data, its legitimacy, which can guarantee public trust, as well as privacy, transparency, and the risks that governments and citizens need to be aware of. These are particularly important for understanding:

- the role of public trust in EU leadership and governments in the adoption of new digital services by citizens
- the conditions under which citizens are willing to accept new digital public services
- the compromises citizens make between privacy and the benefits of using new digital public services in different areas

Trust is essential in situations of uncertainty and interdependence. In the digital environment, these two factors are of paramount importance, and building and maintaining trust is one of the biggest challenges of digitalisation. From an individual's perspective, confidence in the digital age is about whether they are willing to spend time, money, or risk revealing their personal data to participate in commercial and social activities and how vulnerable they become if their data is used to monitor their behaviour, discriminate, or violate their privacy. For organisations, trust means that to take advantage of the digital transformation, each organisation assumes a certain level of risk regarding potential digital security, privacy and consumer protection incidents.[5]

In the European Union, public trust is governed by a combination of laws, regulations and ethical guidelines designed to ensure transparency, accountability and integrity in the activities of public officials and institutions. This includes measures to prevent corruption, conflicts of interest, and requirements from disclosing financial and other relevant information. The European Union's commitment to transparency and accountability ensures that public officials and institutions are held to the highest standards of integrity. Public trust is regulated at the national level, as the EU has no competence to regulate public trust issues. However, the EU has the power to set minimum standards to protect citizens' rights and has adopted various directives and regulations. These directives and regulations are intended to ensure a minimum level of protection across the EU in consumer rights, data protection and competition law. Trust is an essential component of the European Union (EU) and its member states. It is based on the idea that member states will work together cooperatively and in good faith to achieve their common goals. The EU is built on the principle of mutual trust, which means that member states trust each other to comply with EU laws and regulations. This trust is essential for the smooth functioning of the EU and is regulated by a number of mechanisms, including the EU Treaties, EU law, and the EU's institutional framework. The EU relies heavily on mutual trust among its

[4] DigitalEurope 2019.
[5] Misuraca et al. 2020.

member states, which is the foundation for cooperation, collaboration and the successful implementation of EU policies and regulations.

The concept of public trust is an important principle in EU law. It is relevant in many areas of public policy. In general, public trust refers to the trust and confidence the public has in institutions, systems and processes that serve the public good. In the European Union (EU) context, public trust is particularly important in issues such as the handling of personal data, the regulation of financial markets and the management of public resources. To maintain public trust, EU institutions and Member States must be transparent and accountable in their actions and respect the rights and interests of citizens. Furthermore, as the digital transformation progresses and the EU takes advantage of technological developments to improve processes, the EU must continue to ensure that citizens' data is treated securely and adequately protected. As the digital transformation progresses, privacy, particularly personal data protection is increasingly becoming a critical factor affecting trust. The EU has recently considered it important to regulate these areas properly to ensure that the trust established is sustainable within the EU. The EU is strongly committed to protecting the privacy of its citizens. To this end, it has enacted several laws and regulations that can strengthen public trust.

Its founding document is the Charter of Fundamental Rights of the European Union (CFR), which is the cornerstone of the EU's commitment to protect and promote the fundamental rights of its citizens. By guaranteeing these rights and freedoms, the CFR contributes to building public confidence in the EU and its institutions by ensuring that citizens feel protected and secure in their daily lives. Furthermore, by ensuring that all EU citizens have equal access to these rights, the CFR promotes equality, dignity and justice for all.[6]

The next very important document for building trust in the European Union is the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council), a piece of legislation to protect the privacy and personal data of EU citizens. The Directive applies to the processing and storing of personal data transmitted over public networks, such as the internet, and requires organisations to obtain consent from individuals before collecting data. The ePrivacy Directive aims to build public trust by ensuring that organisations handle personal data carefully and that individuals control their data. This includes the right to know what data is being collected, how it will be used, and the right to erasure. The ePrivacy Directive will help promote a culture of transparency and accountability in using personal data, which will contribute to an overall increase in public trust in the EU. By creating a single set of rules across the EU, the ePrivacy Directive will ensure that organisations are held to a higher standard when collecting and storing personal data. It also assures individuals that their data is handled securely and responsibly.[7]

The Law Enforcement Directive [Directive (EU) 2016/680 of the European Parliament and of the Council] is another important piece of EU legislation that provides specific protection for personal data in law enforcement. It applies to law enforcement agencies and

6 Charter of Fundamental Rights of the European Union.

7 Directive 2002/58/EC of the European Parliament and of the Council.

other government bodies that process personal data for law enforcement purposes. The Law Enforcement Directive lays down several basic requirements for processing personal data, such as openness, purpose limitation, data minimisation, and data protection by design and by default. In addition, the Directive ensures the rights of data subjects, such as the right access to and the right to modify personal data and protection against unlawful access and use. In addition, the Directive contains many safeguards to protect personal data, such as the requirement of prior authorisation and appropriate security measures and the obligation to respect the concept of proportionality. In other words, the personal processing of data for law enforcement purposes must be necessary and proportionate. Overall, the Directive provides a comprehensive framework for protecting personal data for law enforcement purposes and is a key instrument for ensuring that the privacy rights of individuals are respected in this context.[8]

The Directive on Network and Information Systems (NIS Directive) [Directive (EU) 2016/1148 of the European Parliament and of the Council] is European Union (EU) legislation that aims to enhance the EU's cybersecurity. The NIS Directive is one of the most significant efforts to increase public confidence in the digital environment. It applies to digital service providers and critical infrastructure operators and obliges them to put in place the technical and organisational safeguards necessary to maintain a high network and data security level. The Directive also requires reporting incidents that compromise the security of network and information systems. By establishing a common EU-wide framework for cybersecurity, the Directive aims to facilitate cooperation and information exchange between Member States and to increase public confidence in the security of digital services. By implementing the Directive, the EU ensures that all digital service providers and operators of key infrastructures are prepared to detect, prevent and respond to cyber security threats. It is a key step towards ensuring public confidence in the security of digital services in the EU and is part of a wider EU effort to promote a safe and secure digital environment. As such, this Directive is important to the EU's efforts to build trust in the digital environment.[9]

The European Union's General Data Protection Regulation (GDPR) [Regulation (EU) 2016/679 of the European Parliament and of the Council] is a comprehensive data protection regulation that gives EU citizens control over their data and its use. It entered into force on 25 May 2018 and replaced the 1995 EU Data Protection Directive. The GDPR applies to all organisations operating within the EU and all organisations processing EU citizens' personal data, regardless of location. The GDPR is a positive step towards protecting the privacy of EU citizens and ensuring that their data is handled appropriately in a way that is trusted by the public. It requires organisations to be open about their personal data collection practices and seek individuals' explicit consent before processing it. Under the GDPR, individuals have the right to access and delete their personal data. In addition, businesses must have appropriate technical and organisational safeguards to protect personal data against unauthorised access, loss or destruction. By enhancing data protection rights and promoting responsible data management practices,

8 Directive (EU) 2016/680 of the European Parliament and of the Council.
9 Directive (EU) 2016/1148 of the European Parliament and of the Council.

the GDPR contributes to developing innovative technologies and services based on the responsible use of personal data and strengthens public trust in the digital economy. The GDPR is a comprehensive regulation that aims to give individuals greater control over their personal data and hold organisations accountable for how they collect, process and manage it. The GDPR also requires organisations to implement systems and processes to manage data responsibly, including security measures to protect personal data against accidental or unlawful destruction, alteration or loss. It also promotes public trust in the digital economy by strengthening data protection rights and promoting responsible data management practices.[10]

These legislations' primary objective is to develop and preserve trust within the EU by protecting personal data. In the vast majority of instances, these procedures significantly restrict the gathering of information, as no individual, organisation, or government may collect personal data without the consent of the data subjects. This indicates that the right to personal data protection should not be violated even if the information is gathered for security purposes and is proportional to the public interest. Therefore, if the user wishes to protect his personal information, this right cannot be prohibited, which is a relatively stringent information-gathering restriction. According to the regulations, if personal information is collected, the user must be informed beforehand and grant his consent. No organisation should place the data subject in a position where he or she is compelled to waive the right to protect personal data concerning this point. In other words, if the data subject does not consent to collecting and processing his or her data, this cannot be prohibited, even for reasons of public interest. This means that organisations must ensure that any data processing is conducted in accordance with the individual's right to privacy and that the data subject is adequately informed of the purpose of collecting their personal data. For example, from a surveillance point of view, it is particularly important to note that some regulations consider the increasing amount of personal data users make available to the public thanks to newer and newer infocommunication technologies and platforms. For example, this is key to obtaining data from open-source information. However, this provision should be interpreted as an acknowledgement of the need to protect the flow of large amounts of personal data into the information space. From an information-gathering perspective, this narrows rather than expands the possibilities. If we analyse the regulations, the protection of personal data is much stronger than the interests of society. Accordingly, the collection and processing of personal data cannot be based solely on the presumption that it is in the public interest, as the EU strongly regulates this possibility and prohibits these type of activities. Overall, consent plays a key role in data collection. From the individual's point of view, consent should be voluntary, unambiguous and independent of any position of power. From the organisation's point of view, it should be proportionate, ethical, necessary, fair and transparent. This requires an appropriate level of trust between citizens and government, and trust and transparency are, therefore, key success criteria for the data-driven government. Therefore, the design and operation of data infrastructures (enabling the sharing and reusing of personal data) should include mechanisms for trust, transparency and privacy to ensure user acceptance. A focus on trust, transparency and

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council.

privacy should be at the forefront of any data-driven government to ensure a successful transition into an era of digitalisation. Trust is essential to the success of any data-driven government, and it should be ensured by providing citizens with clear information on how their personal data is used.[11]

In addition, it is important to note that these legislations do not cover activities related to national security, so if the information-gathering activity falls into the same category, personal data may be collected. In this case, however, the whole legal issue changes if data collection has a national security basis. This specific case will not be examined here in the analysis of the legal background, as it is not closely related to the general surveillance of citizens. A similar exemption applies to the exercise of public authority. The regulations also provide an exemption for crime prevention and detection activities. The key point is that the law does not apply to national security activities. Although this leaves a large loophole in terms of what can be done in terms of data collection, it does protect citizens from having their data collected for purely malicious purposes. The legal situation surrounding data collection activities is complex, and the lines between what is legal and what is not can be blurry in certain cases. The European Union is trying to regulate this properly to build up the right level of trust within the Union in accordance with these regulations. The new regulations aim to ensure that personal data is only collected, used and stored when there is a legitimate purpose. The above legislation and regulations show that the European Union aims to have a strong legal framework to protect data collection activities, which significantly builds public trust.

Social Credit System, the data enabled, morally based, high-tech public administration

China has introduced the constitutionally based Social Credit System (SCS) project in full operation from 2020, and its use is mandatory for all residents and permanent residents of China. The Chinese National Development and Reform Commission (NDRC) was made responsible for the development of the national implementation of SCS. Its primary objective is to develop a centralised data infrastructure that allows the integration and search ability of different profiles and databases, furthermore, previously existing public and private social credit platforms. In 2015, the NDRC started to build the National Credit Information Sharing Platform, integrating the assessment and database of private credit systems of 50 private data providers (like corporates and banks), 42 central government and 32 local government bodies. Going into more detail, this consists of the judicial and criminal information, consumption data of daily goods, traveling or taxation, and market giants' mandatory public data reporting mechanism, which monitors users' online activities. E.g. the Ant Financial platform of Alibaba Group and its Sesame Credit or Baidu (provides search engine, social media platforms) and Tencent Holdings Ltd.'s (provider of WeChat application) Tencent Credit. From the practical to technical point of view, the construction of the SCS is based on comprehensive data collection mechanisms

[11] Wimmer et al. 2020.

through the physical surveillance of natural persons, e.g. CCTV, fingerprint scanners and facial recognition systems, and the analysis of their digital footprint utilising artificial intelligence (AI) machine learning (ML) and Big Data analysis technologies and the elimination of pseudonymisation and anonymisation of digital services in practice and by law.[12] Social Credit System is a robust public administration project with multiple moral aims and a diverse set of rules and criteria, which seeks to whiten the economic system and increase social credibility, safety and soundness. The moral criteria of the Social Credit System identify four desired behavioural standards to increase social cohesion and strengthen trust between people:

1. honesty in government affairs (政务诚信)
2. business fairness (商务诚信)
3. social decency (社会诚信)
4. judicial integrity (司法公信)[13]

Within these four categories, the SCS regulates social behaviour using personal reputation (both online and in person) and material means by generating a unique credit score for each person. It is important to note that, there are different credit points (i.e. several subsystems within the SCS project): government affairs credit, judicial credit, social credit and commercial credit.[14] Along these score levels, 'blacklists' (people with a low score, who are considered harmful to society) and 'redlists' (appropriate, society-building examples of people with a high score) are set up on provincial administrative level. Empirical research by an international team of researchers has revealed that there are 273 blacklists and 154 redlists across provincial levels, which has a flexible scoring methodology, including coronavirus epidemic-related norms and regulations. Researchers concluded that these black and redlists mainly prioritise scores consisting of law enforcement and industry regulations-related activity. Nevertheless, they identified redlists that rewarded political and moral behaviour.[15] In addition to the public listing of persons (with their real personal data) with red and blacklists, the SCS has also assigned a system of rewards and penalties to certain scores in the various credit systems. For instance, high commercial scores could indicate the person's business is eligible for discounted loans and be exempt from paying a deposit or advance payment. Meanwhile, low points would make people face e.g. travel restrictions (not eligible to buy airplane tickets) and restrictions on rent, scholarship, and job opportunities due to judicial, social and government affairs credit scores.[16] Overall SCS is a morally based administrative system built on massive government surveillance and data analytics technologies.

Over the years, in its early stage, SCS has received a lot of concern and negative criticism from the international press and rights defender organisations, including Human Rights Watch. The latter has not only accused the SCS of violating privacy and personal rights, but has also published a report on the violations of minorities rights in China (such

12 Liang et al. 2018: 415–453.
13 Kovalovszki 2019.
14 Liang et al. 2018: 415–453.
15 Engelmann 2021: 78–88.
16 Lee 2020.

as the Uyghur minority) through the Social Credit System and its interconnected law enforcement platform, the Integrated Joint Operations Platform (IJOP, mandarin: 一体化联合作战平台) and Police Cloud application. The report drew attention to the risks of faulty machine learning, namely that the data analysis outlines possible or suspected patterns of behaviour (so-called "unusual activity" trends) of persons who were previously identified as "risky" rather than reacting to actual events and activity regarding that people. This may result in a violation of the rights of the person concerned.[17] However, the original intent of the platform and application was to enhance public safety and political security by setting up an alert for the overconsumption of certain goods like chemicals and other dual-use goods, which can be combined to create IEDs or other homemade weapons. Both systems could become an effective tool for tracking government adversaries, organised crime networks, or even terrorists because it also can establish trends and visualise patterns of relationships through Big Data analysis.[18]

It is a remarkable fact that China has built the enforcement of its restrictive measures that were applied during the coronavirus epidemic on the infrastructure of the SCS. For example, the health Barcode System generates three types of QR codes (which serve as access codes for public transportation) on people's smartphones based on a daily questionnaire assessing travel information and general symptoms of infection. The generated QR codes stand for green, which indicates healthy and allows travel; yellow, which imposes a quarantine obligation (e.g. on arrival in a new province or following infection) and red, which indicates a case of contact or infection (and naturally quarantine obligation) and may as well generate a notification to the relevant public authorities in case of severity.[19] This use case demonstrates that the goals and moral purpose of this high-tech public infrastructure can be customised at any time, setting an example of development for regimes around the world.

Kostka summarised the diversity of the Social Credit Point System's operation as simultaneously achieving the promotion and enforcement of social behaviour in line with the communist state party's views through total control and the fine-tuning of the Chinese-style market economy model also the transparency and higher reliability of civil rights.[20] According to these findings, Social Credit System has the potential and ability to increase the CCP's political sturdiness all over China through indirect economic and moral influence. This set-up is also theoretically more acceptable to society compared to the use of hard repressive instruments of power and because of the following traditions and status quo of power:

- The cultural and political heritage of the People's Republic of China lay the background of moral governance and authoritarian means.[21] However, that does not mean that society is not ready to go beyond that.
- Along China's geostrategic and geopolitical regions, the largest population density and the country's economic centre are in the coastal area. The social stability of

17 Human Rights Watch 2018.
18 Wang 2018.
19 Lin–Hou 2020: 1–8.
20 Kostka 2018.
21 Salát 2009.

this territory is crucial for leadership. Meanwhile, the design and construction make the SCS the most efficient and cost-effective in highly populated urban areas. Yet, the great defence policy dilemma of the Chinese leadership is that this specific geographical area is the most vulnerable by the sea.[22]

- The Chinese-type market economy was created by a social contract created as a result of the status quo after the failed Cultural Revolution and the Tiananmen Square massacre.[23] In simple terms, in exchange for the restriction of political rights (compared to European standards) citizens expect economic growth and a continuous increase in their standard of living. Economic performance is linked to the system's stability, but it also creates an opportunity for the richest market players to develop a new power field.

In a Chinese-type market economy, there has always been the possibility that the most influential and wealthy market players could slip out of government control. Large IT companies (Jack Ma's Alibaba Group, Pony Ma's Tencent Holdings Ltd.) in China and other giant companies that dominate several market segments (Didi) have been collecting data almost limitlessly. However, these data sets were not always fully available to the government. The companies' business interests, reputation and own development ambitions sometimes clashed with the CCP's economic and political policies, for example, concerning the U.S. stock market entry of Ant Financial or Huawei's trust-related security issues that caused a loss in the market margin of manoeuvre. Serious tensions have been triggered in the public–corporate relationship by data leaks on the internet, involving vast amounts of Chinese citizens' personal and highly sensitive data. The excessive data collection practices and inadequate data protection measures and storage procedures of large companies can be held liable for the data breach.[24]

In response to this situation, the CCP, building on the foundations of the system laid down in the 2017 Cybersecurity Act, enacted the Data Security Act at the beginning of 2021, which sets out a security framework for large companies to manage data. In addition, from November 2021, the Chinese Data Protection Law was issued, which mainly focuses on setting up responsibilities and introduces framework regulations aimed at the private sector to archive more reasonable and limited data usage. It contains the opportunity to place data protection fines of up to 50 million yuan (approximately 7.7 million USD or 2.9 billion HUF) 5% of its annual cash flow and expect the appointment of a responsible person for data protection. The law regulates the use of AI-powered CCTV face-recognition cameras in public places, describes the legal basis for data collections, and sets out extraterritorial rules on data transition. Chinese firms shall store data on the mainland; otherwise, a risk assessment shall be conducted with the involvement of Chinese authorities.[25]

[22] Stratfor 2012.
[23] West 2015.
[24] Mészáros 2021.
[25] Kaszián 2021.

SWOT analysis

By examining the EU legislation and directives on trust, the authors have conducted a SWOT analysis to identify the strengths and areas for improvement in efforts to build trust within the EU. For the strengths, the fundamental focus was on the right legislative environment and the existing frameworks, which clearly show the potential of the current conditions. The disadvantages, on the other hand, are those areas that are not properly regulated and, therefore, may have a negative impact on the development and maintenance of trust in the EU and its Member States. Furthermore, the resulting threats were also identified, which could jeopardise the digitalisation process and its potential by negatively impacting people's sense of security and their right to privacy and personal space. The results are shown in Table 1.

Examining the Chinese reforms and the Social Credit System, the SWOT analysis looked at the economic benefits of the credit system and its impact on the population from a state perspective. The opportunities have been examined in terms of the positive impact that the system could have on government and the public. For weaknesses and threats, it looked at how the huge amount of data collected could damage the daily lives of individuals, the economy and affect trust in government. The results are shown in Table 2.

Table 1: SWOT analysis of trust and privacy in the European Union

Strengths	**Opportunities**
• Strong data protection regulations, such as the General Data Protection Regulation (GDPR), prioritise individuals' right to privacy and control over their personal data. • The data protection culture is deeply rooted in the EU, with a long history of data protection that goes back decades. • A commitment to privacy as a fundamental human right and an important aspect of digital sovereignty. • A strong legal framework to protect privacy and respect individuals' privacy rights. The strong data protection regulations and the commitment to privacy as a fundamental human right are seen as positive aspects that contribute to the overall protection of privacy in the EU. Furthermore, the long history of privacy protections and a culture that values privacy also highlights the importance the EU places on this issue. These strengths suggest that the EU has a well-established framework for protecting privacy and ensuring that the privacy rights of individuals are respected.	• The growing importance of privacy and security in the digital age, as consumers become more aware of the risks associated with sharing personal data online. • The rise of new technologies and business models can enhance privacy protections and increase public trust in the digital economy. • Increasing cooperation and collaboration between the EU and other countries on privacy and security issues can help create a more consistent and effective global framework for privacy protection. The opportunities indicate the potential for development and improvement in the sector. The growing importance of privacy and security in the digital age, and the emergence of new technologies and business models that enhance privacy, are seen as good developments that can boost public confidence in the digital economy. Moreover, increasing cooperation and coordination between the EU and other nations on privacy and security issues can create a more coherent and effective global framework for privacy. These prospects indicate that sustainable growth and progress in the European Union's trust and privacy protection is possible.

Weaknesses	**Threats**
• Data protection laws are not uniform across the EU (different Member States may have different legislation), making it difficult for companies to comply with multiple regulations. • Lack of public trust in technology companies and how they handle personal data. • Difficulties in enforcing data protection rules, especially for cross-border data transfers (for manufacturers outside the EU, EU rules are only recommendations, not mandatory). • Data security vulnerabilities can lead to data breaches and privacy violations (data loss, unauthorised access due to supply chain failures may reduce trust). The weaknesses reflect some of the challenges and limitations in the EU's current state of privacy protection. The lack of uniformity in privacy laws across the EU and the difficulty in enforcing privacy regulations can create difficulties for companies trying to comply with multiple sets of regulations. The lack of public trust in technology companies and vulnerabilities in data security also raises concerns about protecting personal data. These weaknesses highlight the need for further efforts to enhance privacy protections and increase public trust in the digital economy.	• The rise of new technologies, such as artificial intelligence and the Internet of Things may raise new privacy and security concerns (there are many areas of the EU's information and communication infrastructures that are dependent on non-EU countries, which can reduce trust in them). • The growing power and influence of technology companies can undermine privacy rights and the ability of individuals to control their personal data (there may be many cases, both at EU and Member State level, where data are handled by a third party outside the EU). • Increased government surveillance and the potential for privacy rights to be eroded for national security purposes. • The growing threat of cybercrime and widespread data breaches and privacy violations. The threats highlighted the challenges that must be overcome to maintain robust data protection safeguards. New technologies such as artificial intelligence and the Internet of Things, as well as the growing influence and power of technology companies can raise new privacy and security issues. In the digital age, the potential for increased government surveillance and the threat of cybercrime both pose significant threats to privacy. These concerns underscore the need for continued attention and action to safeguard the privacy rights of EU citizens, which are essential to maintain trust.

Source: Compiled by the authors.

Table 2: SWOT analysis of the Chinese reforms and the Social Credit System

Strengths	**Opportunities**
• Through the system of scores, listing (publicising) and accompanied benefits consumers can be influenced as well as the development or production goals of businesses. Therefore, the economy can be fine-tuned on political-economic expectations of the CCP. • SCS is able to whiten the economy and increase transparency in certain government matters, which improves the relationship of the people, the market and the government. • Utilising the fear from defamation or desire of praise by the disclosure means of the SCS the expected system-loyal behaviour of citizens can also be achieved with the soft instruments of power. The above statements are explained by the Tiananmen power status quo in addition to the geopolitical situation supplemented with the tradition of moral governance.	• China could be the winner of the new, data-driven technological revolution by its advantage on data collection practices. • The reduction of online anonymity and data analysis capabilities may be able to predictively prevent accidents, violations and crimes. • The creation of a morally customisable, data-based governing model. The possibility for almost unlimited data collection in the public interest is created by legislation as described by the introduction of the SCS. Private sector service providers' practices are based on continuous data analysis, although the new Chinese Data Protection Law seeks to limit this. The health barcode case study also supports the above propositions.
Weaknesses	**Threats**
• Personal data protection is regulated on high level approach. • It is difficult to limit the activities of internal market companies in terms of data provision and cooperation with authorities, so the chance of enforcing extraterritorial scope is low. • The almost unlimited scope of data collection in SCS entails a huge infrastructural burden and a requirement for data storage capacity which financial resources must be continuously secured. • SCS can make the fabric of society inflexible. The review of the Chinese law on data protection assesses the weaknesses in the legislation framework. Meanwhile, the listed fundamental problems of the SCS can be drawn from the urbanisation status and economic weight of China's coastal regions. The above allegations are also backed up by case studies of data breaches by large Chinese companies and by conflicts due to the CCP's economic policies. The weaknesses of the system were highlighted by the interviewees' personal experiences and their perceptions of its social impact.	• There may be many cases where data are handled by a third party outside of China. • The training of the SCS's analysis algorithms or its false positive alerts may cause infringement of rights. The correction of inaccurate data sources could be difficult. These cases provoked a lot of criticism from the international community, damaging China's image. • It can cause psychological damage to individuals that cannot be measured yet and create dividing-lines of trust in society and increase the suppressed aggression toward the government. This creates an environment that is highly receptive and vulnerable for hybrid threats. The SCS's four desired behavioural standards to increase social cohesion and economic prosperity – described in the introduction – is not fulfilled in cases published by international human rights organisations due to technology-related errors. These instances are undermining the international image of the state, which affects the opportunities for global corporations in the trust-based IT markets. The identification of potential threats associated with mental health state and social issues are also supplemented by the deductions drawn from the responses of the interviewees.

Source: Compiled by the authors.

The SWOT analysis shows that the foundations of the EU system are well-regulated and seek to cover all areas that can contribute to building trust. As trust plays a very important role in the EU, the legislators pay serious attention to protecting personal data. Consequently, data protection and security laws have been a part of the EU's policy for several years. The legislation aims to give citizens control over their own personal data. By requiring that personal data be adequately protected, the legislation seeks to ensure that individuals can trust EU institutions and organisations with their information. In contrast, in China, the Social Credit System does not address personal data protection (mostly at the state level) but does not aim to build trust in the government. As a result of people's different ways of thinking, the government there relies much more on acceptance, which means that the population involuntarily agrees to the system collecting and analysing data about them on an ongoing basis.

As the EU has a relatively well-regulated set of manufacturing requirements to produce certain technological devices, it is quite easy to build trust in devices manufactured in the EU. However, this picture is overshadowed by the fact that there are many areas where it is inevitable that the necessary equipment is sourced from outside the EU. For these devices, there is not always a guarantee that the manufacturer has complied with EU rules, reducing confidence in the service or application. This can lead to a lack of trust from customers, who are not sure that the device they are using complies with the EU's stringent manufacturing requirements. In contrast, China typically uses devices and systems manufactured in-house, which means significantly less exposure. The biggest problem is that much data is being collected; storing and processing is a major challenge for the government. Another problem is that the public is not fully aware of what data is being collected about them and the depth to which it is being analysed. In the long term, this can create a lack of trust in the public, which can negatively affect the perception of the government.

Interviews

The semi-structured interviews were conducted with young academics (under 30 years) with expertise in public administration and research on China, who have personal experience of the Social Credit System. The first set of questions asked whether the system had had any impact on their daily lives during their time abroad and what their experiences had been. The next step was to examine the elements and characteristics of the Chinese society that make the social credit system acceptable and workable and how its application affects the four trust target areas (identified in the design of the data-based governance structure). The following questions examined the impact respondents perceived the social credit system to have had on the Chinese economy. In the final section, we looked at what interviewees think trust means in a data-driven Chinese society and what differences they would highlight compared to the European GDPR-based system. Furthermore, respondents see the possibility of a Chinese-style data analysis system being acceptable in the EU. Four people were interviewed during the study, and the following results were obtained from their responses.

The interviewees typically said that it was only an indirect experience and that it had mostly no impact on their daily lives during their stay, which lasted from two weeks to a year. However, they subconsciously had a risk-averse attitude based on some perceived or real norms. This is referred to as the "chilling effect" in the literature. Interestingly, one respondent said he had looked into the issue with Chinese friends who were very positive about the scheme. This may be due to the basic reasons of discipline, respect for tradition (e.g. a child supports a parent in old age, if not, he risks social exclusion), the high level of digitalisation, and the historical traditions (including decades of authoritarianism), the atomisation of society, the lack of a really strong political opposition, the possibility of using good points to move up in society. Overpopulation and high population density require using new, modern tools to achieve more effective crime prevention or other desirable social goals. Due to its non-democratic set-up, the state has many more resources and data than other states. If the state is to be a good steward, it must harness and benefit from this surplus of resources and data. The application of the social credit system is transforming justice and social/business relations. The retrievable data can now be used to create prejudice against another person. The power of the state or the system that allocates the points is increased, but at the same time, the desire to deceive and manipulate the system is increased, thus refining the methods of perpetration. The fear of negative consequences makes citizens more prudent. According to interviewees, the system appears to impact the Chinese economy positively. Everyone has to have a mobile phone; everyone pays with it, cash is becoming scarce, and payment apps track all spending and status, making it easier to check creditworthiness, which has likely whitened the economy. The system also rewards easy consumption and encourages citizens to consume more. This gives more work to developers and more work to analysts and causes less unemployment. It has also acted as a further stimulus to domestic consumption growth. At the same time, it can hinder the conclusion of certain services and deals, making the economy (and social mobility) more rigid.

In a data-driven Chinese society, the concept of trust is more linked to the state, and since the totality of past actions determines it, there is no question that a person cannot be identified or can only be identified for a necessary period. The point here is precise: the data is tightly bound to the person and is widely accessible. Therefore, citizens are confident that the Chinese state will use the data it acquires exclusively for public purposes, ultimately increasing their welfare. However, the state is not accountable to citizens, so the system's transparency is very limited.

- the purpose of the data collection is not specified
- the state can collect data almost without limit
- facial recognition systems and other new technologies make it easier to identify individuals

The GDPR is much more restrictive on the powers of data controllers and processors, while the Chinese regulation is much more permissive. Therefore, a Chinese-style data analysis system is certainly not acceptable; EU citizens typically have a low tolerance for covert restrictions, while China has "discipline". According to interviewees, the current model would face many legal and moral obstacles in the EU. However, to take advantage

of the benefits offered, the main elements of the filtering system could, in their view, be made more flexible with legal and/or constitutional guarantees.

Conclusion

The research confirmed the importance of building and maintaining trust within the EU. The legislative environment has been designed accordingly, and legislators have done their utmost to create situations in all walks of life that are conducive to building trust. The strongest of these is the area of personal data protection, which is extremely well regulated in the EU and its Member States. However, the legislation does not yet strictly regulate the packaging requirements for devices from non-EU manufacturers, nor are the rules for data handling outside the EU fully developed. Accordingly, the first hypothesis was considered to be confirmed.

The Chinese Communist Party has also begun to show a similar attitude to that of EU member states regarding data collection by IT companies and other giant corporations in the state-market relationship. The common feature is that China has also implemented a data protection law that limits the scope of data collection and seeks to force international companies to cooperate with the authorities and provide data security guarantees.

The most striking difference between the two data protection cultures is how they relate to the data subjects' natural persons. The European Union legal framework focuses on the protection of the privacy of the data subject and is designed to impose guarantees of trust and confidence from data controllers and processors. Meanwhile, the data management culture of the Social Credit System requires trust expectations from both the natural persons (the data subjects) and the market actors (the data controllers and processors) to create a secure environment for the public system to operate in which both actors, the company and the natural person, can prosper and develop. This puts the public perspective, not the individual, at the heart of data protection in Chinese data protection culture. These have shown that these types of systems do not address personal data protection and are therefore not applicable in environments such as the European Union, where privacy is a high priority.

References

Charter of Fundamental Rights of the European Union (2012) C 326/02.

DigitalEurope (2019): *A Stronger Digital Europe.* Brussels. Online: www.digitaleurope.org/wp/wp-content/uploads/2019/02/DIGITALEUROPE-%E2%80%93-Our-Call-to-Action-for-A-STRONGER-DIGITAL-EUROPE.pdf

Directive (EU) 2016/1148 of the European Parliament and of the Council (6 July 2016) concerning measures for a high common level of security of network and information systems across the Union.

Directive (EU) 2016/680 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data by competent

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive 2002/58/EC of the European Parliament and of the Council (12 July 2002) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Engelmann, Severin – Chen, Mo – Dang, Lorenz – Grossklags, Jens (2021): Blacklists and Redlists in the Chinese Social Credit System: Diversity, Flexibility, and Comprehensiveness. *AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 78–88. Online: https://doi.org/10.1145/3461702.3462535

Human Rights Watch (2018): China: Big Data Fuels Crackdown in Minority Region. *Human Rights Watch*, 26 February 2018. Online: www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

Kaszián, Ábel Gergő (2021): A GDPR kínai „unokatestvére" – avagy a kínai adatvédelmi törvény megszületése és várható hatásai. *Jogi Fórum*, 20 September 2021. Online: www.jogiforum.hu/publikacio/2021/09/20/a-gdpr-kinai-unokatestvere-avagy-a-kinai-adatvedelmi-torveny-megszuletese-es-varhato-hatasai/

Kostka, Genia (2018): China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval. *Merics*, 17 September 2018. Online: https://doi.org/10.2139/ssrn.3215138

Kovalovszki, Kartal (2019): A kínai társadalmi kreditrendszer [The Chinese Social Credit System]. *DiploMaci*, 11 April 2019. Online: https://diplomaci.blog.hu/2019/04/11/a_kinai_tarsadalmi_kreditrendszer

Lee, Amanda (2020): What Is China's Social Credit System and Why Is It Controversial? *South China Morning Post*, 09 August 2020. Online: www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

Liang, Fan – Das, Vishnupriya – Kostyuk, Nadiya – Hussain, Muzammil M. (2018): Constructing a Data Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy and Internet*, 10(4), 415–453. Online: https://doi.org/10.1002/poi3.183

Lin, Leesa – Hou, Zhiyuan (2020): Combat Covid-19 with Artificial Intelligence and Big Data. *Journal of Travel Medicine*, 27(5), 1–8. Online: https://doi.org/10.1093/jtm/taaa080

Maurtvedt, Martin (2018): *Surveillance and Social Manipulation: A Solution to "Moral Decay"?* Master's thesis. University of Oslo.

Mészáros, R. Tamás (2021): Annyi adatot gyűjtöttek, hogy a Kínai Kommunista Párt is megijedt tőle [They Collected so Much Data that even the Chinese Communist Party Was Scared of It]. *G7*, 25 July 2021. Online: https://g7.hu/vilag/20210725/annyi-adatot-gyujottek-hogy-a-kinai-kommunista-part-is-megijedt-tole/

Misuraca, Gianluca – Barcevičius, Egidijus – Codagnone, Cristiano (2020): *Exploring Digital Government Transformation in the EU. Understanding Public Sector Innovation in a Data-Driven Society.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/480377

Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the

free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Salát, Gergely (2009): *A régi Kína története.* Budapest: ELTE Knfuciusz Intézet. Online: https://btk.ppke.hu/uploads/articles/772735/file/regikinatortenete_teljes.pdf

Stratfor (2012): The Geopolitics of China: A Great Power Enclosed. *Stratfor,* 25 May 2012. Online: https://worldview.stratfor.com/article/geopolitics-china-great-power-enclosed

Wang, Maya (2018): Cambridge Analytica, Big Data and China. *Human Rights Watch,* 18 April 2018. Online: www.hrw.org/news/2018/04/18/cambridge-analytica-big-data-and-china

West, John (2015): China's Political Predicament. *Asian Century Institute,* 30 September 2015. Online: https://asiancenturyinstitute.com/politics/979-china-s-political-predicament

Wimmer, Maria A. – Neuroni, Alessia C. – Frecè, Jan Thomas (2020): Approaches to Good Data Governance in Support of Public Sector Transformation Through Once-Only. *Electronic Government, EGOV 2020, Lecture Notes in Computer Science.* Cham: Springer. Online: https://doi.org/10.1007/978-3-030-57599-1_16

Contents