CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Cyber Considerations for Military Mobility

Henrik Beckvard
Philippe Zotz

Introduction

The importance of military mobility, the ability to transport units, equipment and supplies efficiently and rapidly, seems to be clear for both NATO and the European Union (EU). This importance is exemplified by initiatives such as the Permanent Structured Cooperation (PESCO) project on military mobility under which 25 EU nations have committed to working together.[1] Under Dutch coordination, Project Military Mobility is a PESCO project concentrating on the movement of military personnel and goods within the EU with a focus on administrative hurdles.[2] Likewise, the 2018 Joint Declaration on EU-NATO Cooperation lists military mobility as one of four areas with a particular aim for progress.[3]

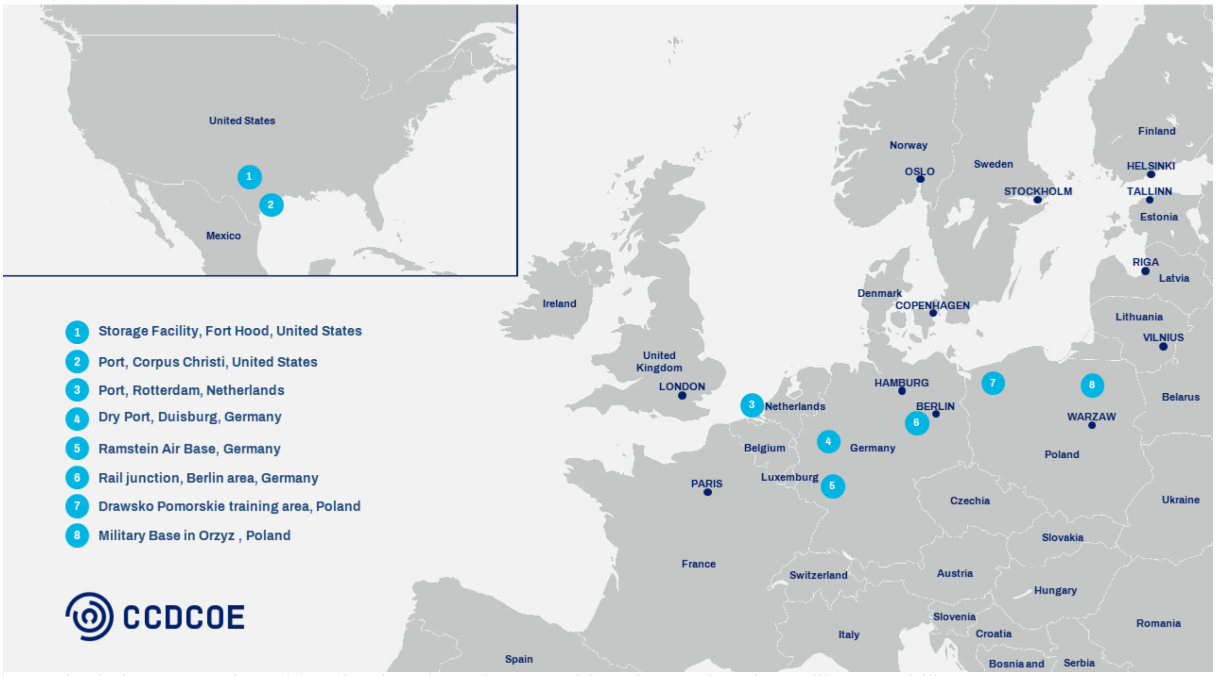
This paper highlights the effects in or through cyberspace that may affect military mobility. It will not give an in-depth or technical analysis, but rather serve as food for thought for areas where cyber considerations should be included in the planning and execution of military mobility operations. Not all issues raised in this paper may be addressed by the military planner alone. Cooperation with relevant partners in cybersecurity, government and industry is often needed. Another essential part of this paper is raising awareness about cybersecurity concerns in military mobility operations for high-level policymakers.

In NATO, the Defender-Europe[4] exercises test the ability of the Alliance to support the large-scale movement of forces across the Atlantic and mainland Europe and exercise Reception, Staging and Onward Movement (RSOM). Military mobility goes far beyond the optimisation of route planning and the provision of personnel and material.

Many factors must be considered when planning for military movement, including whether a ship will be able to use a given port facility, whether the bridges along the suggested route will support the weight of a heavy tank transporter, or if the tunnels are wide enough for a given type of vehicles to pass through. Other factors such as weather and the need for force protection must also be considered. Adding to these are cyber considerations that must be given due attention during planning and execution.

An obvious challenge arises from reliance on civilian infrastructures, given that peacetime transport channels are used by the civilian population. As critical infrastructure may be Government Owned, Government Operated (GOGO), Commercially Owned, Commercially

[1] Council of the European Union. 2017. 'Council Decision Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States.', https://www.consilium.europa.eu/media/32000/st14866en17.pdf
[2] Permanent Structured Cooperation (PESCO). n.d. PESCO PROJECTS MILITARY MOBILITY (MM). https://pesco.europa.eu/project/military-mobility/
[3] The President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation. 2018. 'Joint Declaration on EU-NATO Cooperation.' NATO.int. https://www.nato.int/cps/en/natohq/official_texts_156626.htm
[4] Defender Europe is a large NATO military mobility exercise, see: https://www.nato.int/docu/review/articles/2020/06/16/exercise-defender-europe-20-enablement-and-resilience-in-action/index.html



Map depicting examples of focal points for cyber considerations related to military mobility.

Operated (COCO) or a hybrid of the two, cooperation between private and public sectors is of vital importance.

Most critical infrastructure is reliant on Information Technology (IT) and technology used to control and monitor infrastructure, devices and processes known as Operational Technology (OT). There is a clear dependency on Information and Communication Technologies (ICT), therefore cybersecurity needs to be part of the planning process. The varied legislation, regulations and procedures of sovereign states may also present a challenge.

While there is an obvious dependency on digital systems for military mobility such as the Logistics Functional Area Service (LOGFAS) or fleet and warehouse management software, there are digital systems that may be outside a planner's sphere of influence. These include a whole range of automated systems such as traffic control systems, automated systems for ships, planes and trains.

To protect the functioning of these systems, the interdependencies of critical infrastructures must be mapped. The power grid and communication networks are obvious examples of critical infrastructure on which almost all critical infrastructure systems rely. Critical Infrastructure (CI) and Critical Information Infrastructure (CII)[5] on which the efficient and rapid deployment of units, equipment and logistics rely must therefore be mapped, together with any vulnerabilities and plans for countering those vulnerabilities. The planner must determine which CI and CII a particular movement would rely on and the consequences of any disruption and whether the vulnerabilities be remediated, mitigated or even accepted.

Threats to CI and CII may be physical and either man-made or natural. However, this paper focuses on the threats occurring in or through cyberspace and the consequences for transport if an automated system were to be disrupted by a cyber incident such as a cyberattack.

The effects of a cyberattack may vary from a temporary interruption of service to actions that would have the same disruptive effect as a kinetic attack. Attacks in and through cyberspace are scalable and may be the preferred means of attack for both state and non-state actors wishing to interfere with military mobility in peacetime or war.

The diversity in national legislation, regulations and procedures may pose challenges in the sense that cyberattacks are not constrained by borders or boundaries, and that varying security

[5] Note: For the purposes of this paper CII is defined as the information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country.

requirements for transport and infrastructures may represent a security challenge.

In this paper, we would like to illustrate cyber considerations for military mobility based on military transportation from North America to mainland Europe as it is done in, for instance, the Defender Europe exercises. This paper does not follow any specific route but seeks to highlight the following focal points where cyber dependencies are common to military mobility: Critical Infrastructure and Critical Information Infrastructure, Storage facility, Sea Transportation, Seaport, Inland Waterway Transportation, Air Transportation, Airports, Rail Transportation and Road Transportation are addressed before the Conclusion.

Critical Infrastructure and Critical Information Infrastructure

Whether conducting military mobility or sustaining ongoing operations or simply conducting daily operations, the military relies on CI and CII. Before addressing specific CI in the following sections, some general points have to be addressed. Although there is no universally accepted definition, CI may be defined as the set of assets, systems and networks (both physical and virtual) so essential that their incapacitation or destruction would have a debilitating effect on a state's national security, economic stability, public health and safety.

For CII, there is also no universally adopted definition but EU Council Directive 2008/114/EC defines it as 'ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (tele-communications, computers/software, Internet, satellites, etc.)'. [6]

IT and OT systems are used to control this infrastructure. When the mission owner and asset owner are not the same, there is a need for coordination. As the infrastructure is most often GOGO, COCO, or a COCO/GOGO hybrid, there is a need to establish close coordination and collaboration between the asset owner and the mission owner. For example, a telecommunications service provider (as a mission owner) could rely on an undersea cable (whose owner would be the asset owner) to provide the telecommunications service (mission) between continents.[7] The telecommunications service provider and the cable owner would need to have clear arrangements for the sharing of responsibilities and maintaining the service. The national authorities in the countries between which the cable runs also need to be factored in.

The question of ownership should always be a decision-making factor and whether the infrastructure belongs to a country or company with ties to unfriendly nations.

Collaboration with key actors, both in the sending nation and in the host nation, is essential. To cover all areas, procedures like a Mission Assurance Process essentially follows three general phases:

1) Mission and asset owners identify assets. During this phase, the mission owner would draw up a Critical Asset List – what is important, and why?
2) A threat, hazard and vulnerability assessment is made. In this phase, the asset owner makes a vulnerability assessment – what are the risks to what is important?
3) Risk management. In this phase the risk decision is made – how should the risks be addressed, and can they be mitigated, remediated or accepted?

As significant inter- and intra-sector dependencies exist within both CI and CII, a whole-government approach is needed and Public-Private Partnerships (PPPs) are required to effectively protect CI and CII from threats. These must be based on trust and information sharing. Trust has to be built up, protected and sustained over value-added experience. Trust is, among other things, founded on robust, broad-based, two-way information sharing.

One instrument used to foster information sharing could be collaboration through Information Sharing and Analysis Centres (ISACs), which help critical infrastructure

[6] Council of the European Union. 2008. 'Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.' Official Journal of the European Union. http://data.europa.eu/eli/dir/2008/114/oj.
[7] Beckvard, Henrik and Keiko Kono. 2019. 'Strategic importance of and dependence on, undersea cables.' (NATO CCDCOE). https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.

owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.[8]

An ISAC could help owners and operators of CI protect facilities, personnel and customers against cyber incidents, physical security threats and other hazards. They may prove invaluable in collecting, analysing and disseminating actionable threat information to members and providing them with the tools to mitigate risks and enhance resilience.

In military mobility, it is impossible to ensure that all CI and CII would always be protected. However, a first step could be to conduct a Mission Assurance Process and make sure that asset owners follow cybersecurity standards such as ISO/IEC 27001 or the United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

Storage Facility

Many storage facilities rely on warehouse management systems (WMS) for inventory control and warehouse operations. The security of warehouses and whether they are protected from external threats should be considered during the planning process.

The effects of a cyberattack on a storage facility may include disruption of operations through denial of service (DoS) attacks, or manipulation of databases causing errors and disruptions in the supply chain. An example would be changing the status of an item that requires maintenance to deliver a faulty item instead of a functional one or changing the quantity or the item itself.

If radio-frequency identification (RFID) or cellular systems are used in inventory control, this data could be interfered with, spoofed or jammed possibly leading to false or no information. Man-in-the-middle (MITM) attacks where an attacker inserts themselves between two parties trying to communicate to eavesdrop or alter the communication could reveal logistical operations data to the attacker or cause issues by interfering.

These examples show the need for automated systems and digitised processes to be protected. This includes points that can be dealt with in advance to be able to react quickly in the event of an incident: redundancy and back-ups of the system, regular safety audits for parts of the OT such as programmable logic controllers (PLC) and their vulnerabilities and education and training of personnel. With automated storage facilities relying on warehouse robots, falling back on manual means of locating items after a cyberattack could prove impossible.

Sea transportation

Large-scale military mobility will have to rely on sea transportation where civilian contractors will be employed to ship large and heavy equipment such as tanks, armoured fighting vehicles and trucks. Essentially, the military (as the mission owner) will employ a shipping company (the asset owner) to move military materiel from A to B. Generally, it will be left to the shipping company how to fulfil the task, including protecting itself against cyber threats.

As more ship-owners and ports adopt digitalisation to optimise operations, the industry becomes more vulnerable to malicious cyber activity seeking to exploit vulnerabilities. The growing number of ships and ports connected to the internet and online applications increases their vulnerability to cyber threats.

Shipping is reliant on many cyber related systems including the Global Navigation Satellite System (GNSS), Global Positioning System (GPS) and Automatic Identification System (AIS). AIS allows vessels equipped with transponders to be tracked and automatically identified by sending data at regular intervals. GPS and GNSSs could be either jammed or spoofed (receiving false signals regarding the position of other vessels), which could influence ship navigation. Ship navigation may be affected by attacks on navigational equipment such as GNSS or the Electronic Display Information System (ECDIS).

Spoofing the AIS would affect the ability of the ship to receive accurate information regarding

[8] Note: For further information regarding the Information Sharing and Analysis Centers (ISACs), see: https://www.nationalisacs.org/

the characteristics of other vessels such as name, type, size and callsign and the nine-digit Maritime Mobile Service Identity (MMSI) that is unique to each vessel. The AIS supplements the ship's radar, which continues to be the primary method to avoid a collision when visual contact is limited. Hacking the AIS signal could mimic the location of an existing vessel or show information about non-existent vessels and thereby create considerable confusion or be used as part of a disinformation campaign.

There are ways to detect both GPS and AIS spoofing or cyberattacks directed against other systems, but the military would have to work closely with the shipping contractor to share information and minimise the risk of incidents interfering with the mobility operation. From a military planning perspective, good practice would be to ensure that the shipping contractor follows the International Maritime Organisation's (IMO) *Guidelines on maritime cyber risk management*[9] or equivalent guidelines.[10]

Seaport

The Sea Port of Embarkation (SPOE) and Sea Port of Disembarkation (SPOD) are also areas where cyber considerations must be considered during the planning process to ensure that the equipment will arrive and transit smoothly through the port facilities and arrive at the right destination at the right time and in the right order.

There are many attack surfaces including the IT systems of the port authorities, the AIS receiver at the port, Vessel Traffic Services (VTS) or Industrial Control Systems (ICS) in the port's OT systems, such as ship to shore cranes and other loading and unloading systems.

Seaports may be GOGO, COCO, or a hybrid. From a military mobility standpoint, there is a need to establish close coordination and collaboration between the asset owner (the port authority) and the mission owner (the military).

The creation of shared cyber rapid response teams (RRT) with port authorities and shipping contractors may be contemplated. Quickly detecting and sharing information on system abnormalities could help mitigate the effects of a cyber incident or cyberattack. Such collaboration requires a high degree of trust and should therefore form part of any military mobility exercise involving contractors and other stakeholders.

In *Port Cybersecurity – Good practices for cybersecurity in the maritime sector* [11] the European Union Agency for Cybersecurity (ENISA) provides a detailed description of cybersecurity threats and challenges and security measures related specifically to port facilities.

Awareness-raising may also be done through simple infographics depicting vulnerabilities and what can be done to remediate or mitigate these. In December 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) published an infographic chart depicting typical *Port Facility Cybersecurity Risks*[12] to show examples of how cyberattacks could affect various aspects of port operations.

Another infographic chart, *Cybersecurity for Maritime Facilities*[13] (May 2019) made in collaboration between the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), the United States Coast Guard, the Customs and Border Protection agency, the Federal Bureau of Investigation (FBI) and the Department of Transportation's Maritime Administration is almost a pocket guide of what to do to minimise

[9] International Maritime Organisation (IMO). 2017. 'GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.' MSC-FAL.1/Circ.3. https://www.gard.no/Content/23896593/MSC-FAL.1-Circ.3.pdf.

[10] BIMCO, Chamber of Shipping of America, Digital Containership Association, INTERCARGO, Interferry, ICS, InterManager, INTERTANKO, IMCA, IUMI, OCIMF, Superyacht Builders Association and WSC. 2020. 'The Guidelines on Cyber Security Onboard Ships, version 4.' https://www.intercargo.org/wp-content/uploads/2020/05/2021-12-23-Guidelines-on-Cyber-Security-Onboard-Ships-v.4.pdf.

[11] Drougkas, Athanasios, Anna Sarri, Pinelopi Kyranoudi and Antigone Zisi. 2019. 'Port Cybersecurity - Good practices for cybersecurity in the maritime sector.' ENISA. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport.

[12] Cybersecurity and Infrastructure Security Agency (CISA). 2020. 'PORT FACILITY CYBERSECURITY RISKS.' https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf.

[13] Cybersecurity and Infrastructure Security Agency (CISA). 2019. 'CYBERSECURITY FOR MARITIME FACILITIES.' https://www.sfmx.org/wp-content/uploads/2019/07/NRMC-Cybersecurity-for-Maritime-Facilities.pdf.

risk and whom to contact for reporting a cyber incident.

Inland waterway transportation

When conducting military mobility, inland waterways, where available, may be considered as a means of transport. Ports, cargo ships, bridges and locks are points of interest for cybersecurity as inland waterway shipping is moving towards digitalisation and dependence on ICT systems. An analysis of trends in inland water transport in the EU highlights technical and logistical innovations and developments.[14] Navigation using AIS and River Information Service (RIS) tracking equipment for inland waterway navigation stands out as a large number of traffic control systems are interconnected and have become critical parts of transport operations. Shipping is dependent on the functioning of IT systems and is therefore exposed to cyber risks.[15] With AIS and RIS systems, any system may be a target of the same type of attack as described in the Seaport section.

If a traffic control system was to be affected by a cyberattack, dams, locks and canal traffic lights could be manipulated to cause congestion or delays possibly leading to accidents. Targeted attacks on the inland waterway transport system can have far-reaching consequences for the entire operation and create a ripple effect. Inland port disruption can be achieved via cyberattacks, which includes GPS jamming and spoofing, malware and phishing and DDoS attacks. A disruption in the inland port infrastructure may affect the supply chain, which could potentially lead to cascading disruptions throughout the network[16] and affects all modes of transportation.

Air transportation

Military mobility, especially when conducted between continents, will rely heavily on air transportation. Strategic airlift and commercial airlines will be needed to transport large numbers of troops and quantities of equipment quickly from, for instance, the US to Europe.

Most aeroplanes used for strategic lift will be fitted with a ‘glass cockpit’ with electronic (digital) flight instrument displays integrating the information systems available to the pilots. Among these systems may be the Flight Management System, the Thrust Management System, the Data Communication Management (Datalink) or Aircraft Communications Addressing and Reporting System (ACARS), the Central Maintenance System and the Flight Data Acquisition System or other systems providing the pilots with real-time information for their flight. To interfere with some of these systems, physical access to a particular aeroplane by the hacker would be required but, although more difficult to target, these systems may theoretically be used as attack vectors for interfering with air transportation.

An attacker may also interrupt mobility by attacking elsewhere such as the Air Traffic Management (ATM) systems that assist aircraft from point of departure to point of arrival. [17] Cyberattacks here would affect air transportation in general and not just individual planes.

From a military mobility planning perspective, the focus should be on the vulnerabilities and secondary routes should be planned where possible. Interference with civilian airspace would also affect military aviation. Knowing the vulnerabilities will help frame the right questions regarding cybersecurity for airlines contracted for the transportation of personnel or equipment. As always, there will be a need for close collaboration between the military and civilian contractors and authorities. As with all military systems, military transport aviation should be protected by the Military Computer Emergency Response Team (MilCERT) but

[14] Benga, Gabriel Constantin, Danut Savu, Sorin Vasile Savu, Adrian Olei and Răzvan Ionuț Iacobici. 2019. ‘Assessment of Trends in Inland Waterway Transport within European Union.’ Advanced Engineering Forum, vol. 34 247-254.

[15] Ibid.

[16] Hossain, Niamat Ullah Ibne, Safae El Amrani, Raed Jaradat, Mohammad Marufuzzaman, Randy Buchanan, Christina Rinaudo and Michael Hamilton. 2020. ‘Modeling and assessing interdependencies between critical infrastructures using Bayesian network: A case study of inland waterway port and surrounding supply chain network.’ *Reliability Engineering & System Safety 198*

[17] Hird, John. 2020. ‘AIR TRAFFIC MANAGEMENT: A CYBERSECURITY CHALLENGE.’ Transport Security International (TSI). https://www.tsi-mag.com/air-traffic-management-a-cybersecurity-challenge/.

close coordination must still be maintained with the air traffic authorities involved in the route chosen.

Airport

Air Navigational Services (ANS), including ATM systems, consist of physical, organisational, information and human assets interacting in assisting planes departing from or landing at airports and the transit through airspace. There are many vulnerabilities to such a complex system from not only physical attacks (such as drones or lasers), but also threats to confidentiality and integrity of data, malicious code or DoS attacks on, for instance, GNSS.[18]

Because of these vulnerabilities, there are ongoing initiatives to make this area more secure. These include The European Cybersecurity for Aviation Standards Coordination Group (ECSCG) and the European Organisation for Civil Aviation Equipment (EUROCAE), ED-153. The latter provides guidelines for Air Navigation Service (ANS) software safety assurance. Other initiatives such as the System Wide Information Management (SWIM) [19] and the new pan-European network service (NewPENS)[20] aim at exchanging information and enhancing the reliability and security of aviation data flows.

In May 2020, the US Department of Homeland Security presented its *2020 National Strategy for Transportation Security* (NSTS)[21] including an aviation security plan. This document also addresses vulnerabilities in the air transport sector.

From the planning perspective, it is important to include people with a detailed understanding of the vulnerabilities connected with air transportation as early as possible in the planning process.

Rail transportation

Rail transportation is a crucial part of large-scale military mobility operations. This necessitates close cooperation between the military and the respective railway authorities. If transportation is conducted in peacetime, the primary use for civilian passengers and cargo must be taken into account.

When it comes to the cybersecurity of the rail network, the military, as a user, depends on the individual country's operators and the national cybersecurity framework.

The railway systems' cyberattack surface has increased with its reliance on wireless communication technologies, commercial-off-the-shelf (COTS) and the internet of things (IoT).[22] Initiatives such as the European Rail Traffic Management System (ERTMS) aim to establish a standard for communication and signalling, management and control. GSM, or LTE links, which allow a link between the train and control centre[23] form part of the attack surface.

Points of communication and command and control would be obvious attack vectors to limit mobility. The US Department for Transportation's *Cyber Security Risk Management for Connected Railroads* mentions eavesdropping attacks, DoS attacks and spoofing attacks as three major threats to Advanced Train Control Systems (ATCS).[24]

[18] Lyngset, Tor Einar. n.d. 'SECURING CRITICAL ATC SYSTEMS AND PROTECTING VALUABLE DATA FROM CYBER THREATS Air Traffic Control.' guardREC. https://www.guardrec.com/blog/securing-critical-atc-systems-and-protecting-valuable-data-from-cyber-threats.

[19] Hird, John. 2020. 'AIR TRAFFIC MANAGEMENT: A CYBERSECURITY CHALLENGE.' Transport Security International (TSI). https://www.tsi-mag.com/air-traffic-management-a-cybersecurity-challenge/.

[20] EUROCONTROL. n.d. New pan-European network service - Securing cross-border network connections and underpins safety-critical applications. https://www.eurocontrol.int/service/new-pan-european-network-service.

[21] Department of Homeland Security Transportation Security Administration (TSA). 2020. '2020 Biennial National Strategy for Transportation Security (NSTS).' https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf.

[22] Schmittner, Christoph, Peter Tummeltshammer, David Hofbauer, Abdelkader Magdy Shaaban, Michael Meidlinger, Markus Tauber, Arndt Bonitz, Reinhard Hametner and Manuela Brandstetter. 2019. 'Threat modeling in the railway domain.' International Conference on Reliability, Safety and Security of Railway Systems 261-271.

[23] Ibid.

[24] Liu, Xiang, Duminda Wijesekera, Zezhou Wang, Matthew Jablonski, Yongxin Wang, Chaitanya Yavvari, Keith Holt and Brian Sykes. Cyber Security Risk Management for Connected Railroads. No. DOT/FRA/ORD-20/25. United States. Department of Transportation. Federal Railroad Administration, 2020.

The risk of unwanted tracking or eavesdropping must be considered during the planning process and execution and its potential impact evaluated.

Road transportation

Roads are an indispensable means of military mobility which interference by cyber means could also affect. If traffic lights were to be manipulated successfully, not only would traffic jams and unexpected delays occur, but the selection of alternative routes could also be influenced by sophisticated manipulation eventually causing a ripple effect. As an example, Dutch security researchers showed that it is possible to trigger red lights over the internet by making the system believe that non-existent bicycles are approaching an intersection. This flaw in the intelligent transport system allowed interference with traffic lights in over ten Dutch cities.[25]

Besides physical attacks, risks to traffic light systems may consist of controller or sensor data attacks. Controller attacks may include methods targeting authentication, DDoS attacks and spoofing and are aimed at traffic disruption, eavesdropping and changing traffic light behaviour. Sensor data attacks may encompass cyberattacks on sensor data such as DoS, eavesdropping, firmware modification and spoofing to invalidate sensor data, disrupt traffic or carry out coordinated attacks.[26]

If the control system of a movable bridge was to be hacked, the road system could be paralysed. Attacks on active traffic monitoring systems are another example of possible interference with military mobility operations. False information about the traffic situation could thereby disrupt the flow of traffic.

With the roll-out of 5G and future technologies, it will be possible to employ autonomous vehicles which may prove a huge asset for military mobility. However, these benefits only exist if the network is not interrupted and the area of movement is covered. Through these new technologies, more vehicles and devices (for instance smart cities and road systems) will be connected and cyberattack surfaces multiplied. The inclusion of cyber considerations in the planning and execution of military mobility, including coordination with civilian authorities, therefore becomes even more important.

Conclusion

These focal points are not exhaustive and while some nations may be better prepared to deal with cyber dependencies, they serve as examples of the importance of factoring cyber considerations into military mobility.

The cyber dependencies described in this paper can be grouped into two layers:

1) The cyber physical layer consisting of the infrastructures themselves (ports, roads, bridges, airports, etc.) and their underlying digital systems: automated systems, tracking and fleet management software, warehouse management systems, traffic control systems, communication systems, etc.
2) The legal/policy layer: policy, agreements and law, bilateral agreements, cybersecurity standards and legal backgrounds for civil and critical infrastructure, ownership and control, etc.

Addressing cyber dependencies by falling back on analogue solutions may seem both pragmatic and efficient, but it may ultimately prove a disadvantage. Having the option to function for a time without digital systems may be prudent but making sure that digital problems have digital solutions will be needed if the benefits of digitalisation are to be fully realised.

Supporting initiatives towards reducing administrative hurdles and promoting common frameworks for a heterogeneous cybersecurity landscape throughout NATO and the EU is important in a well-functioning civil-military collaboration for the use of civilian critical information infrastructure assets.

A clear analysis and mapping of vulnerabilities that factors cyber considerations into the planning process should become the norm. This

[25] Greenberg, Andy. 2020. 'Dutch Hackers Found a Simple Way to Mess With Traffic Lights.' WIRED.COM. https://www.wired.com/story/hacking-traffic-lights-netherlands/.

[26] Li, Zhiyi, Dong Jin, Christopher Hannon, Mohammad Shahidehpour and Jianhui Wang. 2016. 'Assessing and mitigating cybersecurity risks of traffic light systems in smart cities.' IET Cyber-Physical Systems: Theory & Applications 1, no. 1 60-69.

encompasses making contingency plans and understanding the roles and responsibilities of host nation authorities and other actors.

Synchromodality – the capability to flexibly adapt transport modes depending on their availability – may be one way of addressing the effects of a cyberattack while remaining reliable and efficient.

With the rollout of 5G and subsequent technologies, military mobility operations will face new opportunities and risks. The interoperability of new technologies and their vulnerabilities must be considered throughout the whole route.

Lastly, the topic of cybersecurity awareness remains central to raising the overall security of any organisation and its operation. Even if a system is designed with maximum security in mind, the human factor should not be forgotten. Therefore, cyber education and training remain fundamental building blocks of cybersecurity where humans may be the weakest link.

Sources

Drougkas, Athanasios, Anna Sarri, Pinelopi Kyranoudi and Antigone Zisi. 2019. ‘Port Cybersecurity - Good practices for cybersecurity in the maritime sector.’ ENISA. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport.

Beckvard, Henrik and Keiko Kono. 2019. ‘Strategic importance of and dependence on, undersea cables.’ (NATO CCDCOE). https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.

Benga, Gabriel Constantin, Danut Savu, Sorin Vasile Savu, Adrian Olei and Răzvan Ionuț Iacobici. 2019. ‘Assessment of Trends in Inland Waterway Transport within European Union.’ *Advanced Engineering Forum, vol. 34* 247-254.

BIMCO, Chamber of Shipping of America, Digital Containership Association, INTERCARGO, Interferry, ICS, InterManager, INTERTANKO, IMCA, IUMI, OCIMF, Superyacht Builders Association and WSC. 2020. ‘The Guidelines on Cyber Security Onboard Ships, version 4.’ https://www.intercargo.org/wp-content/uploads/2020/05/2021-12-23-Guidelines-on-Cyber-Security-Onboard-Ships-v.4.pdf.

Council of the European Union. 2008. ‘Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.’ Official Journal of the European Union. http://data.europa.eu/eli/dir/2008/114/oj.

Council of the European Union. 2017. ‘Council Decision Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States.’

Cybersecurity and Infrastructure Security Agency (CISA). 2019. ‘CYBERSECURITY FOR MARITIME FACILITIES.’ https://www.sfmx.org/wp-content/uploads/2019/07/NRMC-Cybersecurity-for-Maritime-Facilities.pdf.

—. 2020. ‘PORT FACILITY CYBERSECURITY RISKS.’ https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf.

Department of Homeland Security Transportation Security Administration (TSA). 2020. ‘2020 Biennial National Strategy for Transportation Security (NSTS).’ https://www.dhs.gov/sites/default/files/publications/2020-06-12_2020-biennial-national-strategy-transportation-security-report.pdf.

EUROCONTROL. n.d. *New pan-European network service - Securing cross-border network connections and underpins safety-critical applications.* https://www.eurocontrol.int/service/new-pan-european-network-service.

Greenberg andy. 2020. ‘Dutch Hackers Found a Simple Way to Mess With Traffic Lights.’ *WIRED.COM.* https://www.wired.com/story/hacking-traffic-lights-netherlands/.

Hird, John. 2020. ‘AIR TRAFFIC MANAGEMENT: A CYBERSECURITY CHALLENGE.’ *Transport Security International (TSI).* https://www.tsi-mag.com/air-traffic-management-a-cybersecurity-challenge/.

Hossain, Niamat Ullah Ibne, Safae El Amrani, Raed Jaradat, Mohammad Marufuzzaman, Randy Buchanan, Christina Rinaudo and Michael Hamilton. 2020. ‘Modeling and assessing interdependencies between critical infrastructures using Bayesian network: A case study of inland waterway port and surrounding supply chain network.’ *Reliability Engineering & System Safety 198.*

International Maritime Organisation (IMO). 2017 MSC-FAL.1/Circ.3. ‘GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.’ https://www.gard.no/Content/23896593/MSC-FAL.1-Circ.3.pdf.

Li, Zhiyi, Dong Jin, Christopher Hannon, Mohammad Shahidehpour and Jianhui Wang. 2016. ‘Assessing and mitigating cybersecurity risks of traffic light systems in smart cities.’ *IET Cyber‐Physical Systems: Theory & Applications 1, no. 1* 60-69.

Lyngset, Tor Einar. n.d. ‘SECURING CRITICAL ATC SYSTEMS AND PROTECTING VALUABLE DATA FROM CYBER THREATS Air Traffic Control.’ *guardREC.* https://www.guardrec.com/blog/securing-critical-atc-systems-and-protecting-valuable-data-from-cyber-threats.

Permanent Structured Cooperation (PESCO). n.d. *PESCO PROJECTS MILITARY MOBILITY (MM).* https://pesco.europa.eu/project/military-mobility/.

Schmittner, Christoph, Peter Tummeltshammer, David Hofbauer, Abdelkader Magdy Shaaban, Michael Meidlinger, Markus Tauber, Arndt Bonitz, Reinhard Hametner and Manuela Brandstetter. 2019. ‘Threat modeling in the railway domain.’ *International Conference on Reliability, Safety and Security of Railway Systems* 261-271.

The President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation. 2018. ‘Joint Declaration on EU-NATO Cooperation.’ *NATO.int.* https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

Abbreviations

ACARS	Aircraft Communications Addressing and Reporting System
AIMS	Airplane Information Management System
AIS	Automatic Identification System
ANS	Air Navigation Services
ANSPs	Air Navigation Service Providers
ATC	Air Traffic Control
ATCS	Advanced Train Control System
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATS	Air Traffic Services
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
COCO	Commercially Owned, Commercially Operated
COTS	Commercial off the Self
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DoS	Denial of Service
ECDIS	Electronic Display Information System
ECSCG	European Cyber security for aviation Standards Coordination Group
ENISA	European Union Agency for Cybersecurity
ERTMS	European Rail Traffic Management System
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FBI	Federal Bureau of Investigation
GNSS	Global Navigation Satellite System
GOGO	Government Owned, Government Operated
GPS	Global Positioning System
GSM	Global System for Mobile Communications/Groupe Spécial Mobile
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IMO	International Maritime Organisation
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardization
IT	Information Technology
LOGFAS	Logistics Functional Area Service
LTE	Long-Term Evolution
MilCERT	Military Computer Emergency Response Team
MITM	Man-in-the-Middle (attack)
MMSI	Maritime Mobile Service Identity
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology
NSTS	National Strategy for Transportation Security
OT	Operational Technology
PESCO	Permanent Structured Cooperation
PLC	Programmable Logic Controllers
PPP	Public-Private Partnerships
RFID	Radio-frequency identification
RIS	River Information Services
RRT	Rapid Response Teams
RSOM	Reception, Staging and Onward Movement
SPOD	Sea Port of Disembarkation
SPOE	Sea Port of Embarkation
UHF	Ultra High Frequency
VHF	Very High Frequency
VTS	Vessel Traffic Systems
WMS	Warehouse Management System