JISR Services

Oude Waalsdorperweg 61
2597 AK The Hague, Netherlands

Telephone: +31 (0) 70 374 3644

The 7th NATO BIOMETRICS TECHNICAL INTEROPERABILITY WORKSHOP

-Report-

Location: Carlton Beach Hotel, The Hague, the Netherlands and Webex;

Timeframe: 30 November – 01 December 2021;

Participants: in total there were 50 participants, of whom 14 were physically present in the conference room, while the others joined the working sessions on Webex. Altogether the attendees were representing:

- NATO Nations: Belgium, Canada, Czech Republic, Germany, France, Great Britain, Hungary, Italy, Netherlands, United States of America. The USA were represented by four specialized establishments:
- Defence Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), Naval Criminal Investigative Service (NCIS), National Ground Intelligence Centre (NGIC), Department of Defence Program Management Biometrics (DoD PM Bio), and US Army Europe and Africa (USAREUR-AF).
- NATO Commands: Supreme Headquarters Allied Powers Europe (SHAPE), NATO Special Operations Headquarters (NSHQ), NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and NCI Agency.
- Partner Organizations: INTERPOL, EUROPOL, European Union Agency for the Operational Management of the Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), Biometrics Institute, The Netherlands Defence University.
- Industry: BSS Unit, HID-Global, HSB, Lakota, Thales, Xator

General Overview: As in the previous iterations, the workshop was organized as an open forum to facilitate consultation and collective demonstration of biometric capabilities in order to assess the completeness of the applicable NATO Standards. The NBTIWS provided a unique opportunity for specialists to demonstrate current interoperable biometrics capabilities and to debate the future development of NATO biometrics interoperability standards.

The results of the workshop were reported at the Senior Level Meeting of the NATO Biometrics Programme Coordination Group (NBPCG), which was organized on 2-3 December 2021, at the NATO HQ.

Day 1- 30 November 2021:

1. *Welcome. Introductory remarks:* Mr. Cristian COMAN from the NCI Agency welcomed the participants and offered the introductory and administrative details. Next, he offered the opportunity to all participants, to introduce themselves.

2. *INTERPOL: Upgrade on biometrics system, biometric HUB and XML data exchange.* As in every year, Mr. Mark BRANCHFLOWER offered to the audience an interesting presentation with regards to the INTERPOL biometric systems and the way ahead. In opening, Mr. BRANCHFLOWER stated that lately, the INTERPOL member nations (i.e. 196 nations) expressed more interest in using the biometrics systems, and they are asking for more

biometric data exchange. He mentioned that there has been a long process going on to upgrade their Facial Recognition System (IFRS) and the Automated Fingerprint Identification System (AFIS), through a partnership with Idemia (i.e. Industry Company). The deadline to finish the upgrade and implement the new versions of IFRS and AFIS is March 2022. Next, he went on presenting briefly the projects "Foxspot" (which deals with collecting biometrics from illegal immigrants and then checked against nations data bases) and "WAPIS"/ West Africa Police Information System (which deals with the installation and implementation of three AFISs in West African countries). Further on, Mr. BRANCHFLOWER stated that the current architecture allows 195 nations to submit biometric data to the INTERPOL through the I-24/7 network, which in the next future will be moved into a cloud. He also mentioned that in the future the IFRS and AFIS will be replaced by the "Biometric HUB". This enhancement will allow for automatic responses between nations and from the INTERPOL Data Base. Mr. BRANCHFLOWER offered an example saying that the negative responses (i.e. no matches) will be pushed back automatically, whereas if there is a match in the system, it will be double checked by a biometric examiner and then sent back to the nation, in no more than 10 hours. The briefer also pointed out that the INTERPOL still uses binary files, but the plan is to replace them with the xml version 6.0, which was implemented already on March 2020. In closing, the Mr. BRANCHFLOWER claimed that the ownership of the data belongs to the member nations which could caveat it (e.g. restrictions to share) or could even request to have the data removed from the biometric systems.

3. *eu-LISA: "Biometric systems/ services built and operated by eu-LISA".* The briefing was presented by Mr. Istvan RACZ, who mentioned that eu-LISA was established in 2011, and it started to operate on 01 December 2012. Mr RACZ mentioned that the Agency's mandate was reinforced with EU Regulation 2018/1726, and that the organization was headquartered in Tallinn, Estonia. The operations division was located in Strasbourg, France, and it also had a liaison office in Brussels, Belgium. There were currently 305 staff working in the eu-LISA, who were either seconded national experts or direct hired. The agency aims to increase its workforce to reach at least 370 personnel by the end of 2022. Next, Mr. RACZ presented the systems currently used for the external border management of the EU, which also contain biometric data – i.e. the Visa Information System (VIS/ is a database containing information, including biometrics, on visa applications by Third Country Nationals requiring a visa to enter the Schengen area), the Schengen Information System (SIS II/ is a database used by 31 European countries to find information/ alerts about individuals and entities for the purposes of national security, border control and law enforcement) and the European Dactyloscopy Database (Eurodac/ is a fingerprint database for identifying and managing asylum seekers and irregular border crossers). As a shortfall, Mr. RACZ mentioned that the three systems were running in parallel and there was no central storage of entries and exits in/ out of the EU. To mitigate this deficiency the EU will fully implement the Entry/ Exit System (EES). The EES will be an automated IT system for registering travellers from third-countries, both short-stay visa holders and visa exempt travellers, each time they cross an EU external border. The system will register the person's name, type of the travel document, biometric data (fingerprints and captured facial images) and the date and place of entry and exit, in full respect of fundamental rights and data protection. The EES will be interconnected with the abovementioned three systems and will exchange information. In addition, from the Biometrics perspective, the four systems (i.e. VIS, SIS II, Eurodac and EES) will be connected via the Shared Biometrics Matching Service (sBMS), which will perform biometric search and matches on fingerprints and

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

facial images. From the technical interoperability perspective, the briefer stated that all systems implemented different versions of the ANSI/ NIST-ITL standard, offering details with regards to fingerprints and facial images support. It is also to note that the biometric files use a binary format. Next, Mr. RACZ presented the quality control business rules for sharing data to the EES. He mentioned that the quality of the shared data is checked at the national level (before submission) and at the EES level (upon reception) according to three categories: biographic data, compliance with the ANSI NIST standard and the raw biometric data.

4. *EUROPOL: Europol and its role in the new EU architecture for information systems for security, borders & migration.* Mr. Krzysztof KLEBEK started the brief presenting EUROPOL's set-up for the international law enforcement cooperation, which included the liaison officers at the EUROPL's headquarters and the EUROPOL's mission worldwide. The main topic of the briefing was about the EU's interoperability programme, which aims at closing information gaps by upgrading EU information systems for security, border and migration management and making them work together in a smarter and more efficient way. The programme is led by the European Commission, includes EU Member States, Schengen Associated States, eu-LISA, FRONTEX and EUROPOL and is built to support the border guards, police officers, investigators, visa officials and migration officers. Mr. KLEBEK stated that the goal was to enhance interoperability by modernising the existing systems (SIS, VIS, EURODAC), by building new systems (EES, ETIAS, ECRIS-TCN), by adding EUROPOL to the new architecture (QUEST) and by "connecting" all with interoperability components (ESP, sBMS, CIR, MID). The briefer mentioned that the interoperability was needed due to a combination of factors, such as: the current systems did not "talk to each other", limited information regarding the entry/ exit data on non-EU citizens, difficulty to access information from non-Law Enforcement systems and limited use of EUROPOL data, which might grant entry to the EU to dangerous individuals. In closing, the briefer presented the new architecture of systems for security, borders and migration purposes, emphasizing the use of biometrics through the newly employed Shared Biometrics Matching Service (sBMS). The biometric data shared through these systems is always owned by the nations, while the EU organizations' role is to facilitate sharing, to perform transactions management and to conduct technical exploitation.

5. *Academia: The use of biometrics in military operations and international humanitarian law.* There were two briefings on this topic, presented by professor Marten ZWANENBURG from the Netherlands Defence University and by Mr. Sebastian CYMUTTA, law researcher at the NATO Cooperative Cyber Defence Centre of Excellence. Mr. ZWANENBURG presented the use of biometrics in military operations from the perspective of the Law of Armed Conflict (LOAC). He focused on two vignettes – Targeting and Capture and Detention. Regarding the targeting, professor ZWANENBURG insisted on differentiating the military targets from the civilian population and objects, in the conduct of military operations. With regards to the capture and detention, professor ZWANENBURG presented the caveats on collecting biometrics from subjects without their consent. In closing, professor ZWANENBURG stated that research on LOAC shows that law may have important consequences for when and how biometrics can be used, while NATO member states do not all have the same obligations, and interpret obligations differently. Next, Mr. CYMUTTA offered an overview of the CCDCOE's project with regards to the data protection within a military context. He mentioned that the basic setup of the project was to deal with the comparison of the different legal regimes covering the use of biometric

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

data and the challenges in processing and sharing them in a multinational context. He went on saying that the intent was to create a comparative study to help understand how NATO member states use biometric data and what are their perceived challenges. To achieve that, three rounds of questionnaires have been circulated via different channels, but since most of the nations consider this information classified, there were almost no returns received. With regards to other upcoming projects, Mr. CYMUTTA mentioned the publication "The rights to privacy and data protection in armed conflict", which is also meant to be a study on the interplay between different legal regimes regulating privacy and data protection in conflict situations. In closing, Mr. CYMUTTA presented three collaborative research efforts for the CCDCOE:

a. Research effort 1 – "Military Data and Information Protection – An EU Perspective", intended to be a collaborative effort between Researchers of the Netherland Defense Academy, NCI Agency and the CCDCOE. The goal of the paper is to bridge technological, legal and practical questions (interdisciplinary approach. While discussing the Law of the European Union, the paper cold potentially serve the facilitation of legal interoperability between the EU and NATO. Completion to be expected in the first half of 2022.

b. Research effort 2 –"Legal Framework for international sharing of biometric information", is intended to be a collaborative paper addressing one of the most discussed topic in the area of military data exchange. The goal is to provide a practical approach to the divers' legal landscape and incite further research on the topic. Completion to be expected in the middle of 2022.

c. Research effort 3 – "Continuing support to NATO exercises". One of the main focal points on this project is to provide legal injects with regards to the International Humanitarian Law. The goal is to integrate legal questions with other aspects (e.g. STRATCOM or technical exploitation) to essentially "train as you fight".

6. *FBI: TEDAC Latent and Intelligence workflow process*. Mrs Jennifer RAYMOND started the FBI briefing with presenting the Terrorist Explosive Device Analytical Centre (TEDAC). The TEDAC was established in 2003 to serve as the single interagency organization to receive, fully analyze, and exploit all terrorist improvised explosive devices (IEDs) of interest to the U.S. and its partners. Next Mrs. RAYMOND explained the latent evidence and examination workflow internally, between US agencies and with foreign partners. Further on, Mr. Jeffrey HANSON explained the workflow process once an Identification notice is received at the Identity Intelligence Team, and the sharing procedures with international organizations (e.g. INTERPOL). The FBI team also shared some successes deriving from collaboration with internal US agencies as well as with international organizations or multiple nations. As such, it was mentioned that to date there were more than 4500 known or suspected terrorists identified due to TEDAC latent prints and DNA. Next, the briefer presented the FBI biometric sharing effort with the INTERPOL via the TREAD project. The purpose of the TREAD project was to issue Blue Notices to INTERPOL for all non-US citizens FBI/ DOD biometrically linked to IEDs and/ or caches. Once a blue notice is issued, all 192 receiving member countries are requested to search the subjects' fingerprints against their known and unknown recipients. To date there have been over 2500 Blue Notices disseminated and there were 35 Blue Notice hits by partners since project TREAD started in 2015. With regards to the future biometric sharing, the briefers mentioned the intent to expand sharing with EUROPOL and other multilateral organizations. From the interoperability perspective, FBI is preoccupied by more automated sharing, possibly

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

over VPNs. At the end of the presentation the briefers offered more examples of successes resulted from the collaboration with INTERPOL and EUROPOL as well as three I2 successes, which had possibly prevented terrorist attacks on US and its partners.

7. *US Defence Forensics and Biometrics Agency (DFBA): STANAG 4715 revision process update and Watch ML format.* Mr. Brian HARRIG presented an update on the STANAG 4715, edition B, ratification status. He mentioned that the NATO Standardization Organization (NSO) had released NATO STANAG 4715 Ed. B for ratification in July 21, and that Nations have until 08 January 2022 to provide comments. Next, he announced the topic of Biometrically Enabled Watch Lists (BEWL). He introduced the notion of "Downstream systems" and defined them as systems that typically do not make biometric transmissions to ABIS, but are responsible for tracking biometric activities within ABIS. He went on saying that STANAG 4715 did not provide methods to manage updates to the BEWL. Next, Mr. HARRIG discussed the US DOD WatchML file specifications. He mentioned that XML files, generated by the Bi2R system, are used to transmit the BEWL metadata to the Biometric Data Management System (BDSM). In addition, there are distinct sets of WatchML files generated for the DoD BEWL or the other custom watch lists. The WatchML is transactional as a new file is generated when an individual's BEWL data has changed. The so called "WatchML Request" files are serialized and can be used to add, modify, refresh, or delete an individual's BEWL information. Mr HARRIG said that the current version 5.0 of WatchML, allows for the BEWL information of an individual to be packaged into a single XML file to enable transactional ability. Then the WatchML Specifications enables multiple identities to be placed in a single file (i.e. enables a BEWL snapshot). He went on clarifying that a WatchML submission to an ABIS does not trigger an ABIS transaction in the same sense as a biometric submission or data base search. He specified that the "WatchML Requests" files prompt updates to metadata in the database and "WatchML Responses" files allow confirmation of receipt.

8. *US National Ground Intelligence Centre (NGIC): I2 workflow process and systems support (BI2R).* The NGIC briefer defined the Identity Intelligence (I2) as being the intelligence resulting from the fusion of identity attributes and other information and intelligence associated with those attributes collected across all intelligence disciplines. He mentioned that the purpose of the I2 was to discover true identities and the connection between these identities and other individuals, places, events, or materials thus analyzing their pattern of life and characterizing their threat. He went on to present the I2 across the full range of military operations, and stated that the I2 provides the "so what" of biometric transactions and that the I2 operationalizes collections. The briefer concluded that the I2 bridges the gap between national, multinational, tactical, operational and strategic operations and homeland defence. Next, the briefer introduced the BEWL and stated that the purpose of the DoD BEWL was to identify persons of interest (POI) at the point of biometric collection by consolidating and integrating regional, functional, Combatant Command and lower echelon POIs biometric data and providing DoD BEWL information to interagency and limited foreign partners in accordance with existing directives and bi-lateral agreements. The speaker went on presenting the advantages of having the watch lists based on biometrics compared to biographic data. He stated that historically, the watch lists had been name-based, and the success or failure of the watch list had relied on a human screener's ability to determine the identity of the person encountered. However, the screeners were tricked many times by the POIs who had hidden their identities by using disguises, aliases and falsified documents. Meantime, improved biometric collection and

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

matching capabilities, have increased the effectiveness of watch lists by turning positive identification into a simple exercise of automated biometric recognition. Next, the briefer offered some details regarding the BEWL alert categories and sub-categories and exemplified their relevancy in the conduct of operations. In closing the NGIC briefer presented the Watch list process starting with identifying the POI and ending with the targeting operation conducted to counter the threat.

Day 2 – 01 December 2021

9. *Defence Science and Technology Laboratory (DSTL): UK Defence Exploitation Facility (DEF):* Mr. Simon MURPHY, from DSTL, presented the briefing and introduced the DSTL to the audience. He mentioned that the DSTL was an executive agency of the Ministry of Defence (MOD) providing world class expertise and delivering cutting-edge science and technology for the benefit of the nation and allies, in the defence and security field. Mr. MURPHY introduced the UK DEF and mentioned that its role is to conduct the level 3 exploitation of materiel and personnel (the level 1 is conducted by troops at or near the incident and the level 2 is performed by specialized personnel at a deployed laboratory in theatre of operations). As the specialized in country facility, the DEF is a capability that enables the exploitation of material and personnel by scientific, technical and specialist intelligence activities in order to deliver timely intelligence. The briefer continued to present the UK DEF structure and capabilities and their contribution to force protection. In closing, Mr. MURPHY offered some successful examples of identifying identities based upon collaborative effort between multiple national agencies and nations.

10. *SHAPE: Considerations for leveraging biometrics to support NATO Operations, Missions, and Activities.* The SHAPE representative, LTC PEREZ-RIVERA presented the briefing which was centered on considerations about the implementation of the NATO Biometrics Framework Policy into NATO Operations. He started from presenting the main requirement which was to identify what the NATO policy frameworks agreed to provide and implement. Next, he spoke about assessing the facts, and commented on the different authorities relevant for leveraging biometrics support to operations, about the data protection requirements and sharing intent. In order to implement the policies, the SHAPE representative recommended few topics for analysis, as follows: how other organizations do the biometric operations, what the NATO stakeholders want to do, what the potential use cases are, based on inputs received from stakeholders, who are the requirements holders and the risk owners, what technical architecture is needed, what sharing agreements are needed, what are the biometric technical business rules, what networks are we needed to be on, is there a need for a cross domain solution, and the “Ping and Ring” implementation at national level. LTC PEREZ-RIVERA also presented some hypothetical use cases with regards to the NABIS implementation into the NATO missions and operations. At the end, regarding the relevancy of biometric operations the briefer concluded that collection might take many forms, from focused biometric collections to site exploitation. Further on he stated that the resultant biometric signatures and captured material would enable the commanders to plan and conduct follow-on operations (eg. Counter Terrorism operations).

11. *BSS Unit: Demonstration: Motion QR/Data QR encryption and authentication of biometric data.* Mr. Andras PATKAI, presented the Data QR technology which is used to transmit and authenticate data. He stated that the technology is based on the 3D QR codes,

which was described as follows: a rapid sequence of QR codes is played back in video format, enabling on-the-fly decoding of large amounts of data and displaying original documents. As long as the data is authenticated at the source (e.g. NABIS, issuing body), the secure distribution of DataQR cryptograms is guaranteed. Authentication is performed on a physically guarded hardware security module (HSM) located in the client's infrastructure. Anyone with a smart phone and the downloaded app can reliably check another person's identity and biometric status, even offline. Next, he mentioned the Data QR benefits, as follows:

a. Security: Combination of asymmetric encryption technologies, including 1024-4096-bit RSA and a transport encryption to carry the public key,

b. Authenticity: Guaranteed by the cryptographic structure,

c. Versatile use: Several documents can be chained into one string (connect biometric or medical data to person, no need to validate and connect two separate documents),

d. Portability: Public keys are distributed widely on mobile devices, app securely updated with public keys released by the issuer (e.g. NATO) on a regular basis,

e. Offline use: Authentication can be performed using offline devices,

f. Flexible: Access levels can be set for modular disclosure of information on a need-to-know basis (Different levels of access may be provided to Homeland Security and Department of Defense),

g. Easily updateable: Document expiry and modifications immediately reflected in system upon central authentication,

h. Privacy: Personal data remains with the subject, is not stored in a central database, no need to share data, users store their own data,

In closing, Mr. PATKAI conducted a successful demonstration on data QR encryption and authentication of biometric data.

12. *NCI Agency: Exercise Northern Spirit 21: Exercise description and outcome.* Mr. Radu CIMPEAN presented the biometrics and Identity Intelligence exercise Northern Spirit 21 (NOSP 21), which took place in Keflavík, Iceland, 18 to 28 October 2021. The exercise demonstrated an increasing appetite for biometrics and identity intelligence, including 42 participants from NATO Nations, Commands and industry. NOSP21 was organized in conjunction with the Counter Improvised Explosive Device (C-IED) exercise Northern Challenge 2021, which was hosted by the Icelandic Coast Guard. NATO's Emerging Security Challenges Division, through the Defence against Terrorism Programme of Work, sponsored both events. The main goal of the exercise was to practise the technical and operational interoperability of biometrics and identity intelligence within a simulated scenario of NATO led operations. The NOSP 21 training audience had the opportunity to work with the NATO ABIS and three other ABIS, brought by Industry, to exercise biometric data import, matching and exchange with the other participating systems. The briefer stated that the biometric transactions were executed between four different ABISs, in compliance with NATO STANAG 4715, ed. B, which constituted a premiere, since it was the first time when three Industry companies and NCI Agency successfully tested together the implementation of this STANAG. Also it was the first iteration when the INTEL FS was employed in NOSP to support I2. The INTEL FS proved to be stable, reliable and enabled the I2 analysts to replicate reality in terms

of collating reports and on conducting evaluation and analysis. Mr. CIMPEAN, presented that NOPS 21 was a successful exercise and that the training objectives were met. In addition, NOSP 21 constituted a premiere on the following aspects:

a. NCI Agency successfully tested with three companies the implementation of the NATO Standardization Agreement (STANAG) number 4715, and managed to share biometric data between the four ABIS present in the exercise;

b. I2 analysts as a training audience. This aspect brought substantial value to the "so what?" of the biometric matches – i.e. the resulted Identity Intelligence which enabled to deny anonymity from threat actors;

c. NOSP 21 running in parallel with NC 21 exercise. Thus NOSP 21 demonstrated the value of I2 and Biometrics to the operational community from NC 21 (i.e. EOD/ IED operators).

In closing, the briefer stated that there are challenges for the future. NOSP 21 lacked scripters both in number and in adequate expertize, especially in technical exploitation for the operational conduct stage. Having key personnel available for the entire cycle of the exercise is paramount to ensure success, and this will be an important test for the next iteration.

13. *Chief LL Team: Exercise Northern Spirit 21: Lessons Learned.* Maj. Francis HUIJGENS, NLD, who was the Chief of the Lessons Learned (LL) Team, presented a substantial briefing on the Lessons identified in NOSP21, which was built together with Ms. Amy Middleton from the UK DSTL. Maj. HUIJGENS stated that a Lessons Learned capability provides a commander with the structure, process and tools necessary to capture, analyze and take remedial action on any issue and to communicate and share results. He also mentioned that from the LL perspective, the NOSP community should consider the following three questions in every stage of the exercise: What worked well?, What did not work well?, and What can be done better?. He went on saying that there were 34 Lessons Identified (LI) captured in NOSP 21, divided in three categories:

a. exercise planning and product development;

b. exercise operational conduct;

c. technical interoperability.

In closing the LL chief presented the way ahead regarding the validation of the captured lessons identified and he also pointed out the top three LI categorized in accordance with the three questions presented above:

a. What worked well? – adding I2 training audience and exercising I2 analysis. Also, having four different ABIS to exchange biometrics data was very well received;

b. What did not work well? – there still are differences in interpretation of STANAG 4715;

c. What can be done better? – deeper integration of the NOSP with the Northern Challenge exercise as well as the employment of a level 2 laboratory to support both exercises.

14. *NCI Agency: Exercise Northern Spirit 21: Technical interoperability.* Mr. Cristian COMAN briefed the audience on NOSP 21 technical interoperability. He started the brief with

the technical interoperability training objectives and then presented the observations and lessons identified throughout the exercise planning phase as well as during the exercise operational conduct. Next, the briefer presented his conclusions, as follows:

a. What worked well?

- four different implementation of STANAG 4715 were tested in an operationally relevant scenario;

b. What did not work well?

- ambiguity in the NATO Standards particularly in the xml implementation;
- the STANAG 4715 does not support the intelligence reporting format;

c. What can be done better?

- provide technical infrastructure to allow testing ahead of the exercise.
- make the dataset available earlier in the exercise for early verification.

In closing, Mr. COMAN presented the following recommendations to be considered for the next iterations of NOSP:

a. improvement to the standard through periodic testing;

b. Implementation Guide and Business Rules will need to be developed;

c. need to address data quality issues (e.g. mismatching between images and metadata);

d. need to test the security aspects;

e. need to test the data ownership aspects (e.g. the delete submission):

- need to deconflict between gateway delete and NDS.

f. data to be more representative and operational relevant;

g. latent submissions were not used during the exercise but this will be useful to do in the future:

- will required latent analyst to be in the exercise;
- could use the UWL or other systems;

h. need to review ahead of time the latent scenario. The STANAG does not properly address how to work with NLS:

- who should look at the NLS, the submitter or the receiver of information?

i. the format of the match report should be included in the STANAG;

j. remove all schemas which are not used (see FBI ebts 11). This will help reducing the number of classes generated from the schema;

k. allow for the NATO Ping Error Message to be used with the Ping Submission and with the Ping Response (e.g. when pushing not when pulling);

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

15. *HSB: Exercise Northern Spirit 21: Conclusions and recommendations.* Mr. Victor van UITERT presented the briefing, which started with a presentation of the HSB Company and then included the HSB's experience in NOSP 21. Of note was the HSB's preoccupation for an Automated Compliance and Verification (ACV) project. The briefer stated that the NATO biometric systems will be developed to assist NATO and NATO nations to share biometric data in accordance with the NATO security policy. ACV is a capability that enforces this by using the Biometrics technical business rules (BTBR) to automate sharing, verify compliance, and audit to ensure biometric data is processed in accordance with national and NATO sharing arrangements. This capability is essential to legal and timely data sharing and will determine the level of success of biometrics in support of NATO operations. Regarding the BTBRs, Mr. van UITERT mentioned that the BTBRs are a set of rules in a system developed to automate the requirements of sharing arrangements. They are used to manage how biometric data records are processed, how long they are stored, and with whom they are shared. They are developed to serve the requirements of data originators. Next, Mr. van UITERT presented the way in which the "Ping and Ring" transactions were conducted during the NOSP 21 exercise. In closing, he provided the following recommendations for the future NOSPs:

a. Improve STANAG 4715 and ACV Compliance

– Develop reference files and validation software

b. Test and audit the ping & ring process with specific attention to the legal perspective

– Describe and implement business rules that respect the GDPR

– Caveat contents must be set and remain intact, to allow traceability

– Usage of the NPS retain flag with sender and receiver

– Follow up NPS + retain and NES submissions with NDS submissions

c. Integrate ACV with 'network bridging' systems

– May require security markup / classification metadata

d. Describe a BEWL sharing process

14. *Lakota: Exercise Northern Spirit 21: Conclusions and recommendations.* Mr. Phillip MERRIT with the solution architecture Lakota brought in the exercise, which involved the API Gateway, the Whorl application and the ABIS Transaction Manager (ATM). Regarding the ATM, Mr. MERRIT stated that it provided implementation of the NATO API Gateway interface and that it received biometric submissions and generated responses in any format. In closing, he presented his conclusions and recommendations with regards to Lakota's participation to NOSP 21, as follows:

a. API Gateway provided a good mechanism to ensure that the systems were interoperable (above and beyond the STANAG);

b. XML Standards bring new challenges which need to be considered;

c. Poor quality and non-standard data is prevalent due to legacy collections and being able to handle poor quality data is important

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

d. Biometrics are looked upon differently by different nations which result in varying requirements about automatic matching and privacy concerns.

e. Having everyone co-located working towards a common goal was a great experience.

15. *Xator: Exercise Northern Spirit 21: Conclusions and recommendations.* Mr. Robert HUBER briefed on the biometric solutions developed by In Cadence, which is a Xator company. He presented the ABIS in a Box, its software capabilities, the Ares Gateway architecture options as well as examples of architecture for ABIS in a Box and the collection devices. Next, he spoke about the capabilities the In Cadence can provide, which included the mobile biometrics kits, the enrolment workstations and the ABIS in a Box. In closing, he offered the technical features of the equipment presented with regards to the biometric data ingested and the biographic information processed.

16. *Exercise Northern Spirit 21: – Live Demonstration: Ping and Ring transactions on* exercise scenario. Mr. Radu CIMPEAN, from the NCI Agency, conducted a live demonstration on “Ping and Ring” transactions, from NABIS to NABIS. The demonstration replicated an use case from the NOSP 21 and could be followed by both participants present in the room and online through the Webex.

Conclusions: The 7th NBTIWS, as the previous iterations, continued to be instrumental for enabling and achieving the appropriate set-up to discuss about the development of the Biometrics Capability in NATO. Whether it was attended by technicians, operational experts or academicians, the NBTIWS allowed for fruitful considerations and debates that aim for a potential implementation in order to improve the technical and operational interoperability. A key take-away was learned from the international partner organizations present at the workshop (e.g. INTERPOL, eu-LISA, EUROPOL) - they all facilitate sharing of biometric data amongst nations, while the nations maintain the ownership of the data. There are more eloquent examples that NATO can inspire from and adapt for proper use. The development of an Identity Intelligence capability in NATO is a must, in order to mitigate the vast array of threats that NATO will be facing in the future. Whether these threats are hybrid, conventional or asymmetric, they all have one factor in common - the complex, volatile and human centric environment NATO will be operating in. Thus, it is also advised to collect requirements and initiate investigation and analysis to develop an I2 application adapted to NATO’s business rules. Further on, it is recommended that NCI Agency conducts research on developing a BEWL version to be tested, experimented and later implemented in operations to replace the current biographic watch lists. Last but not the least, it is highly recommended to continue with the Northern Spirit exercise, which is the only known collective training opportunity on Biometrics and I2 in NATO. It constitutes the perfect venue to test, experiment and validate Biometrics and I2 concepts, business rules and scenarios that could later support contingency operations.

As final note, the NCI Agency, being the host of the NBTIWS, expresses its sincere appreciation to all the Nations, NATO Organizations and Industry that were present and contributed to the success of this event.

Drafted by: Radu CIMPEAN
Viewed and Endorsed by: Cristian COMAN

NATO Communications and Information Agency
Agence OTAN d’information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int