NATO STANDARD

AComP-5637

PROTECTED CORE NETWORKING (PCN)

Edition A Version 1
DECEMBER 2019

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED COMMUNICATIONS PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

10 December 2019

1. The enclosed Allied Communications Publication AComP-5637, Edition A, Version 1, PROTECTED CORE NETWORKING (PCN), which has been approved by the nations in the Consultation, Command, and Control Board (C3B), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 5637.

2. AComP-5637, Edition A, Version 1, is effective upon receipt.

3.

4. This publication shall be handled in accordance with C-M(2002)60.

for Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 PROTECTED CORE NETWORKING (PCN)

1.1. INTRODUCTION

1.1.1. Network Enabled Capability (NEC), a concept similar to network centric warfare, is a way of performing military operations that is appropriate to the current and future operational environments. The requirements for technology support are large, mainly focused on providing solutions for effective sharing of information and flexible, widely available communications, the first depending on the latter.

1.1.2. Protected Core Networking (PCN) is a concept used to establish a flexible but secure military transport infrastructure to support military operations based on NEC. A network based on PCN offers high IP transport availability, efficient resource sharing, resilience and defence against cyber-attacks.

1.1.3. PCN provides the specifications required to interconnect efficiently different national network segments so as to formulate a global, core network while at the same time ensuring a minimum level of security and qualitative of services. Specifically, PCN attempts to address the following challenges: first, provide an increased number of potential interconnection points in a static as well as in a federated mission environment by reducing the number of the resources and the time required; secondly, to simplify the procedures of interconnecting to such a network under various scenarios or use-cases (e.g. static, deployed or mobile ones); finally, to guarantee a specific level of availability and quality of services, while offering cyber-defence capabilities.

1.2. TARGET ENVIRONMENT AND APPLICABILITY

1.2.1. PCN is an overarching concept; it is applicable to both the Static and the Deployable (networking) Domains, as well as their interconnection. As the Deployable Domain can be considered as an extension of the Static one (connected through satellite links or otherwise), applying different concepts in either domain would negatively impact the overall efficiency. For this reason, the development of a common set of interoperability specifications to support connections to either Domain is needed.

1.2.2. Although a Federation of Networks (FoN) in the Static Domain is mainly a homogeneous construct of individual networks and information domains with higher availability and bandwidth than those in the Deployable Domain, static networks may equally suffer from deliberate cyber-attacks and/or unintentional outages. Besides, it can be expected that the amount of traffic traversing the networks in the Static Domain is higher than in the Deployable one and thus, the non-availability of links or elements of the Static Domain may equally impact operations and day-to-day business.

1.2.3. On the other hand, despite a main line of effort in mission networking is focusing on the Federated Mission Networking (FMN) concept, mission networks may come in different flavours depending on the participants and the requirements that are applicable to them. This may lead to additional requirements as far as PCN is concerned.

1.2.4. The set of PCN STANAGs provides a baseline that is applicable to both static and deployable FoNs, but it does not exclude any other additional specifications should a situation requires this.

1.3. OPERATIONAL REQUIREMENTS

1.3.1. The operational requirements that led to the establishment of the PCN concept, the definition of the PCN architecture and the corresponding Interoperability Specifications (ISpecs) are the following:

1.3.2. Efficient infrastructure sharing: Multi-national operations have become the standard model for modern military engagements. Many nations contribute, and all bring parts of their national infrastructure for support. For several reasons (e.g. national requirements or lack of common interoperable standards), these infrastructures cannot be interconnected leading to a large number of redundant networks, as well as to waste of resources (e.g. RF frequencies). This would impact the global agility of the deployment in terms of size weight and power and resource provisioning. In addition, mission infrastructures are typically set up to facilitate information between the various coalitions, e.g. NATO, Mission, and CIMIC. Many of these infrastructures are typically idle while at the same time others are in dire need for more capacity. The inability to interconnect the infrastructures leads to a deployment that is inefficient and expensive both in terms of initial investment cost and maintenance cost. Hence, the network-centric nature of business models nowadays affects not only the NATO Enterprise but also the Alliance as a whole. This requires the interconnection of NATO Enterprise and NATO-nations networks, creating a Federation of Networks both in the Static domain and in the Deployable domain, by sharing efficiently the available network infrastructure.

1.3.3. High reliability: When supporting a NEC environment, it is critical that communications are available to all entities. Inability to share information would lead to uncoordinated actions, possibly with disastrous results. In order to achieve a highly reliable communications network, the network must not only be protected against random failures, but also against targeted attacks, either physical or cyber-attacks. Current communication networks often achieve the latter by isolation, but this is not a viable option in an NEC environment where information must be shared with coalition

partners. In such a case, high availability of the offered communication links and services must be ensured by other means like efficient resource sharing.

1.3.4. Support of dynamic and federated environments: PCN is not a static network. Although it is expected that it will be based mainly on the interconnection of independent, static networks, it will also interconnect with deployed ones so as to extend its reachability and offer connection points and end-to-end connectivity to federated missions. The ultimate goal is to support dynamically changing federated environments by requiring minimum or no adaptations regarding their interoperability capabilities.

1.3.5. Seamless relocation of information domains: Agility of military entities has been identified as a key enabler for modern operations. Two important factors for this have been addressed above: the high reliability of the communications network, and the extensive reach of the network enabled by sharing of infrastructure. However, in order to fully reap the benefits, military entities must be able to geographically move and reconnect without needing a technician to reconfigure anything. The military entity must be able to focus a 100 percent on the mission rather than dealing with technology. This seamless relocation, and in some cases connectivity on the move, needs requirements for a PCN Interoperability Specification (ISpec) to fully reach the desired agility.

1.3.6. Converged networks: Shared awareness in an operational setting is difficult to be achieved, and a variety of sensors and inter-human communications are needed to support this objective. This means that transferring of images, live video streams, command and control applications, voice calls, teleconferences, and videoconferences are all useful services to achieve shared awareness. To maintain agility, these must be easily accessible to the users through one network connection.

1.3.7. Efficient utilisation of communication links: Communications links come in a variety, and not all links are suitable for all purposes. For example, an Internet link can provide high bandwidth, but is not a very reliable one and therefore, it cannot be used in many systems. In order to create a flexible network that is easily reachable, it is important to be able to use all available resources, but at the same time to ensure that the required security properties and Quality of Service (QoS) requirements are satisfied. This provides the best support for the various users of the communications capability.

1.3.8. Automated risk management: Constructing a communications infrastructure that is flexible and at the same time provides high availability guarantees to the users can be challenging, even in fairly simple environments. Once complexity and dynamics are added, it becomes a true challenge. Maintaining high availability for the users

means quickly understanding the risk of failure and attacks, and strengthening the network accordingly.

1.3.9. Federated management: A federated capability is characterized by collaboration between independent entities rather than a common authority and direction. Managing a federated communications infrastructure is therefore a matter of properly managing the individual components and having the components collaborate. Since an overview of the full, federated capability is still needed, e.g. for mission planning and execution, the components must share certain information to allow the build-up of a high-level all-inclusive view.

1.4. PCN PRINCIPLES

1.4.1. To address the operational requirements described in the previous chapter, the following PCN principles are defined:

1.4.2. Establishment of a federated by nature network: PCN addresses the efficient infrastructure sharing operational requirement, by being federated in nature. The concept of an expanding core is applied to increase the PCN range and at the same time make user domains smaller and therefore more agile. In other words, PCN is designed for a federation where multiple partners interconnect and are able to share infrastructure, under both static and deployed scenarios, without losing control of their national components or any of the required security properties. This means that one communication infrastructure can be used by information domains at different classification levels, as well as by different nations. However, since a nation retains control over its national contribution, it can choose to only share idle capacity, or to prioritize critical national traffic.

1.4.3. High availability: A network built on PCN principles using a shared interconnected environment is likely to achieve higher availability than an isolated network due to the additional redundancy offered in a way similar to the Internet model. Moreover, PCN includes specifications particularly aimed at increasing the availability of the network by using specific control mechanisms and protecting from network failures and targeted attacks, such as Denial of Service (DoS) cyber-attacks. This principle aims at addressing the high reliability operational requirement.

1.4.4. Implementation independent: In a federation, systems are built by sovereign entities and are used for a variety of tasks, typically including participation in coalition operations. Since the systems are not under common direction or under a common authority, it is not possible to mandate a certain system implementation as it would not fit all the national needs. The approach must follow the interface specification approach as recommended in the NATO Network-Enabled Capability (NNEC) Feasibility Study (FS). This way, nations can implement networks as needed, or adapt legacy networks,

while being fully interoperable with coalition partners in a federated setting. To this end, clear interoperability points (IOP) with specific requirements are adequately defined while leaving the internal implementation details to the Nations. Automation of the connection mechanisms at the interfaces supports dynamic and federated environments, as well as seamless relocation of both users and PCN networks.

1.4.5. Efficient network utilisation: In PCN the properties of the link are captured and the use of the link is tailored accordingly. The link properties are further used to analyse the overall quality of the network to identify potential problems. Users signal their QoS and their traffic protection requirements when using a PCN network and the path through the network is based on them. This results in an efficient utilisation of communication links.

1.4.6. Differentiated services, resource management and precedence handling: PCN supports various traffic classes (e.g. video streams, interactive voice calls, etc.) and treats traffic with diverse security or QoS requirements differently. However, when a resource is shared between different users, there is a danger of exhausting it with insignificant traffic, while important messages are being dropped. PCN addresses this issue by supporting multiple precedence levels to ensure that the most important traffic is delivered even when the bandwidth is scarce. Moreover, mechanisms are used to manage the resources efficiently so as to ensure the best usage of the available ones. Precedence handling and resource management are combined with Service Level Agreements (SLAs) with the users. The SLAs set forth an agreement between a PCN network and the users on e.g. the minimum allocated bandwidth, the precedence levels to be used, etc. This principle, in combination with the efficient network utilisation address the “efficient utilisation of communication links” operational requirement and contribute to the “converged networks” ones.

1.4.7. Situational awareness sharing and federated management functionalities: High availability of the core network is, among else, a result of shared awareness between the different elements of the network with respect to capabilities, current resource utilisation and cyber defence. While PCN does not mandate how a national component of a PCN network is built or managed, it sets minimum characteristics on the management and the way the components exchange management-related information to allow the necessary collaboration for support of operations. This ensures that it is possible to generate global views of the federated communications infrastructure without necessarily getting the details of every component. Exchanged information includes performance and security information about all parts of the infrastructure, such as available capacity of links, error rates, security properties, as well as information about the traffic load, and cyber-attacks. Knowledge of user requirements through the SLAs complements the picture and adds to the awareness of what to deliver. This principle contributes to the “high reliability”, “federated management” and the “automated risk management” operational requirements.

1.4.8. Resilience and cyber-defence capabilities: PCN protects the availability with respect to both (unintentional) failures as well as targeted cyber-attacks1 (e.g. Denial of Service attacks). Protection mechanisms are pervasive in PCN, ensuring that resources are used appropriately and that unauthorised traffic is blocked immediately without consuming network resources. To maintain a low risk, automated risk assessment continually feeds the network management and operators to ensure proper awareness. PCN requires that the components of a PCN network are able to automatically assess the risk related to availability. This can be achieved by examining the link properties of the various communications links, and evaluating any redundant paths that add robustness to the network. Decision support components of the management system further advice operators to what the best way forward is in a given situation. Any identified weaknesses can then be addressed by the network operators, e.g. by adding additional redundant links, or by adding security measures to improve the reliability. This principle addresses the “automated risk management” operational requirement and contributes to the “high reliability” one.

1.4.9. Network management and cyber defence integration: Cyber defence, defined here as the protection against cyber-attacks, is an important capability in modern infrastructures. However, network management and cyber defence are typically separated and both communities construct their own situational pictures and can potentially both make changes to the network based on actual events. In a network where availability is a primary objective, cyber defence and network management must be integrated in order to ensure a common situational understanding and coherent actions in response to events. This principle contributes further to the aforementioned situational awareness sharing, as well as to the “automated risk management” operational requirement.

1.5. OVERARCHING ARCHITECTURE

1.5.1. As explained, Protected Core Networking (PCN) is a concept used to establish a flexible but secure military transport infrastructure to support military operations offering high IP transport availability, resilience and defence against cyber-attacks.

1.5.2. PCN creates couplings between information domains and the transporting infrastructure. Its purpose is to provide high service availability by optimising the usage of the available resources regardless of the threat environment.

1.5.3. Within a coalition environment various information domains exist, which range from national, to NATO and coalition ones, each running at their own security level. To interoperate these domains and efficiently share information, where allowed, it is

[1] An attack may be a cyber-attack but could also be a physical attack (e.g. taking out a node, network component by physical means).

necessary to have their networks physically interconnected and share the same transport infrastructure, rather than rolling out separate transport networks for each network and each security level or domain.

1.5.4. The PCN Overarching Architecture is depicted in Figure 1.

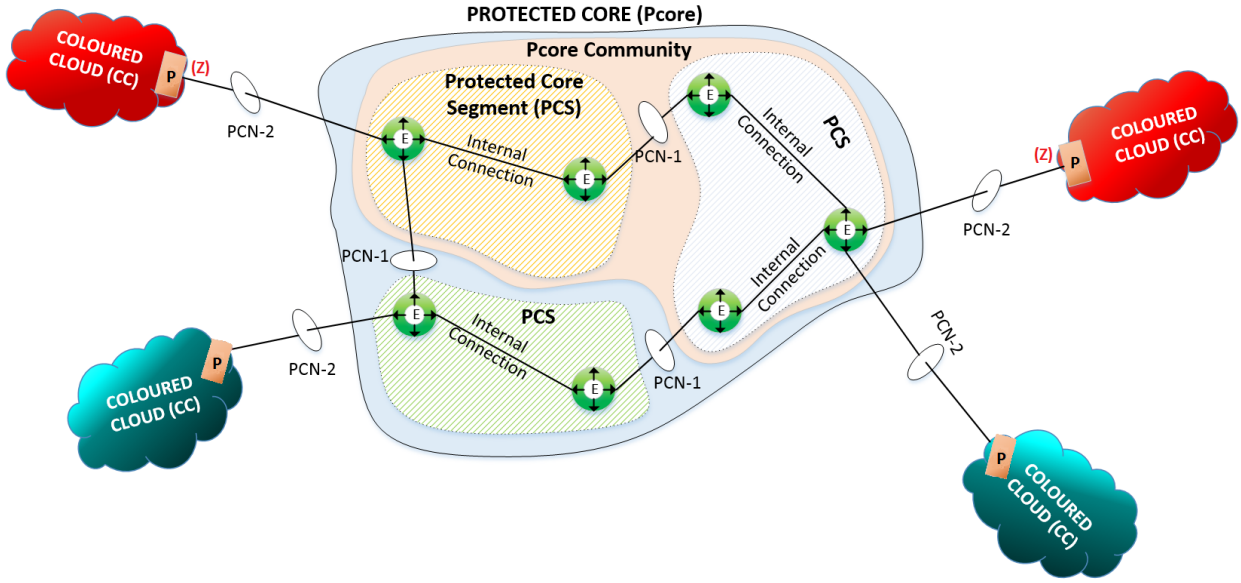

Figure 1: The Protected Core Networking (PCN) Overarching Architecture

1.5.5. A PCN consists of a number of elements described below [RTO AC/323(IST-069)TP/424, 2012]:

a. Protected Core Segments (PCS-es): A PCS is a network built on the principles of PCN as described in section 1.4 and designed to work seamlessly with other PCS-es in a federation of systems. Each PCS shall satisfy a set of functional requirements, called PCS characteristics, to support the PCN concept.

b. Protected Core (PCore): A PCore is a set of PCS-es working together in a federation of systems approach to collectively achieve the characteristics of PCN. That is, PCore is the overall core federated network offering protected infrastructure sharing, the elementary network elements of which are PCS-es.

c. PCore Community (PCC): A community of PCS-es that share common interests at the same security level (e.g. a particular mission) and intend to work more closely together. PCC-es are a subset of the PCore.

d. Coloured Cloud (CC): A CC is a cloud of a specific information (security) domain. If information confidentiality for the traffic transported between CC-es is needed, crypto devices (Z) shall be used to tunnel traffic via the PCore. In such a case, these crypto devices (Z) are part of the corresponding CC-es; PCore does not offer information confidentiality.

e. PCN-1: PCN-1 is the service interoperability interface point between PCS-es in a PCore. PCN-1 is used for service delivery and to share all necessary management information between PCS-es.

f. PCN-2: PCN-2 is the service interoperability interface point between CC-es and PCS-es. PCN-2 is used for service delivery and service management to CC-es.

g. Enforcement nodes (E): These are logical component of a PCS at which the PCS-es interconnect with each other and where CC-es are connected to the PCS-es. An E-node supports PCN1, PCN-2 or both.

h. P-node: Edge node of a CC, which is connected via PCN-2 to one or more E-nodes.

i. Internal connections (or internal links) are connections used for traffic forwarding between E-nodes of the same Protected Core Segment. As they are within one administrative domain (the PCS), they do not have to adhere to strict interoperability standards as connections between E-nodes of different Protected Core Segments (i.e. a PCN-1 connections). Nevertheless, internal connections have to conform to some minimum requirements to adhere to PCS characteristics. On the other hand, the security objectives for internal connections are the same as for PCN-1 and PCN-2 links.

1.5.6. All links that interconnect E-nodes (i.e. PCN-1 and internal links) or links that connect users to E-nodes (i.e. PCN-2) shall be capable of being carried over various carriers (having e.g. LOS, BLOS, or IP transport capabilities, etc.).

1.5.7. Both PCN-1 and PCN-2 interfaces support the transport, connection and management services. The requirements for each Interface are reflected in the corresponding STANAGs: PCN Core Specifications STANAG 5638, PCN Static Specifications STANAG 5639 and PCN Deployable Specifications STANAG 5640. Some of the requirements of PCN-1 and PCN-2 are identical whilst others are unique to either one.

1.5.8. PCN aims at negating any threat (intentional and/or unintentional) that limits users' access to the transport services of the network. This applies to both real-time, near-real time as well as to non-real time services.

1.5.9. PCN shall interwork with existing legacy network implementations e.g. Black Core Routing Networks (BCR). This can be achieved in different ways. The simplest one is to use the legacy networks as a carrier for PCN interfaces (PCN-2, PCN-1, PCS Internal Links). In this case there is no interoperability between the legacy networks and PCN services. However, this will be a popular option as multiple nations and NATO are expected to build PCN over existing network infrastructure. The second option is when interoperability is required between hosts connected to PCN services (PCN-2) and hosts connected to legacy BCR services. In this case, the use of an interoperability solution between the PCN and the legacy network will be necessary. This solution must ensure that the PCore security is not compromised (especially the authenticity of the packets in the PCore) as well as handle any other interoperability constraints like QoS adaptation, service level requirements, reconciliate the IP addressing plans either based on non-overlapping addressing plans, or based on address translation/NAT, etc.

1.6. BENEFITS

1.6.1. The high-level benefits obtained from the aforementioned PCN principles and architecture are summarised in the following paragraphs.

1.6.2. High availability. This is achieved by offering increased redundancy due to the shared interconnected infrastructure, the applied resource management, the controlled, authenticated access, as well as the federated and integrated security and network management. In addition, the use of traffic classes in combination with QoS requirements and precedence handling ensures that even in case of internal congestion, critical traffic will still be delivered. Finally, automated risk management further enhances the network availability by foreseeing potential issues and dealing with them promptly.

1.6.3. Flexibility and agility. The applied converged network but implementation independent approach, as well as the offered plug-and-operate capability which allows seamless relocation, will enhance both flexibility and agility of the Deployable Units. Furthermore, by fully automating the connection process, the military entity (which can be anything from a soldier to a large headquarter) can concentrate on the primary task and use the communications capability without delay.

1.6.4. Deployment in a cost-effective and time-efficient manner. While the high network availability is likely to provide the most needed operational requirement, sharing of infrastructure is likely to provide the greatest financial benefit reducing deployment cost significantly. Deployable Units will have the capability to plug-and-

operate their equipment to pre-existing PCN infrastructure in a timely manner and to share resources with other participants.

1.6.5. Increased collaboration capabilities. The Converged Network approach enables services like live video streams, command and control applications, voice calls, teleconferences, and videoconferences to be easily accessible to all users through one network connection. Moreover, the effective allocation of resources ensures the delivery of these services irrespective of the current network conditions. The interconnection of the users employing these services enhances operational collaboration capabilities at all levels.

1.6.6. Increased security awareness and robustness against cyber-attacks. The inherent security PCN capabilities which will be described below, increase significantly the security level of the offered services in comparison with isolated, ad-hoc national networks. These inherent PCN capabilities render PCN network(s) resistant to DoS and other cyber-attacks.

1.7. OPERATIONAL DEPLOYMENT PROCESS

1.7.1. The operational flexibility provided through the use of the PCN concept is depicted in the following example of a multi-national deployment involving a federation of three nations. This example is used to show the operational deployment process and the corresponding phases. While all associated diagrams depict a single information domain for simplicity, it should be noted that a PCN infrastructure is agnostic to the information domain of the attached users / Colour Clouds.

1.7.2. The consideration of the operational scenario begins at the strategic level. Figure 2 shows three PCS-es. In the case that one of the “nations” is actually NATO, the corresponding PCS represents the NATO Communications Infrastructure (NCI). Otherwise, each PCS represents that nation’s sovereign infrastructure network, equivalent to the NCI for NATO. While not shown in the diagram, the transmission bearers between E-nodes within the infrastructure of the PCS-es will generally be provided by public telecommunications operators (PTOs) either as generic Internet access or leased lines.

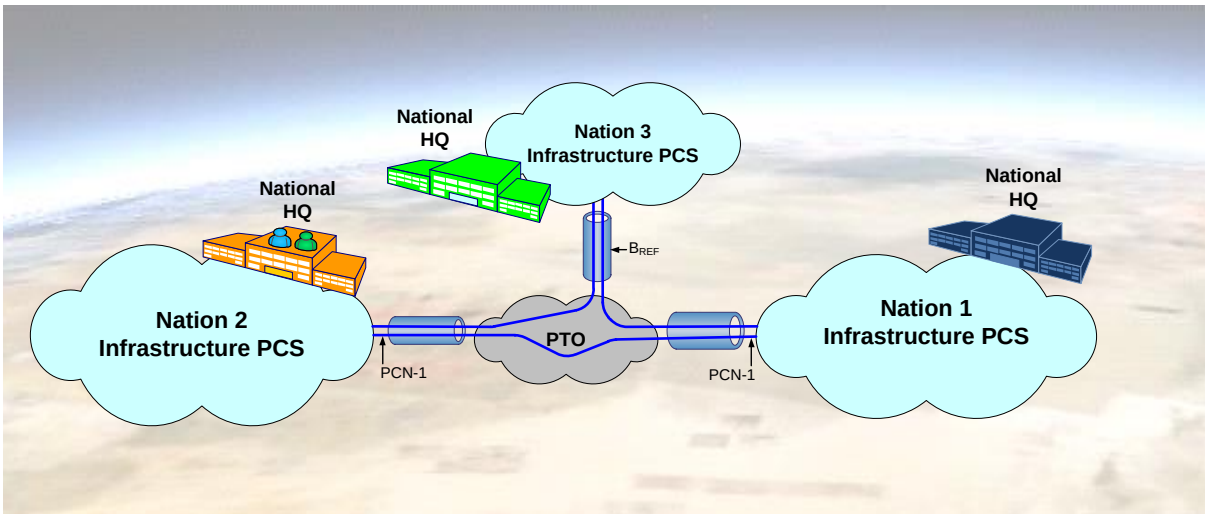

Figure 2: Strategic Decision Phase

1.7.3. The interconnection of the infrastructure networks is made via a mesh of interconnected PCN-1 interfaces that, in this particular example, are carried over transmission capabilities provided by a PTO. PCN requires that one side of the PCN-1 interface assumes responsibility for the provision of bearer capabilities, so in this example the PTO may in fact be two or more PTOs. The collection of these three interconnected PCS-es can represent a Protected Core Community (PCC), which facilitates guaranteed levels of Quality of Service (QoS) at strategic level between any Coloured Cloud communities attached to one of these PCS.

1.7.4. PCN supports users of all domains. A NATO SECRET CC community is established between CC-es within each National HQ across the three infrastructures, enabling remote consultation between the three Nations in order to setup the SECRET infrastructure dedicated to the mission. PCN support for end-user mobility allows any Nation's representative to be able to log into their home systems, through the infrastructure PCC, from within any other Nation's HQ. This is illustrated in Figure 2 via the physical presence of representatives from Nation 1 and Nation 3, embedded in the National HQ of Nation 2 for a physical conference to assist the mission planning.

1.7.5. The following key decisions are taken by the three nation federation during mission planning:

- Nation 1 and Nation 3 will roll out their deployment by sea;
- Nation 2 will deploy from the air;
- Nation 1 (day zero) and Nation 2 are each allocated a Zone of Responsibility, for which they must provide the main deployed communications infrastructure, including a reach-back capability in each case;
- Nation 1 would provide the maritime communications infrastructure; and

- Nation 3 would provide force support to both Nation 1 and Nation 2, but will rely heavily on their respective communication infrastructures.

1.7.6. Following these decisions, Nation 1 establishes a maritime PCS. Each naval platform represents an E-node capable of supporting multiple information domains across a PCN-2 interface. These PCN-2 interfaces will normally be carried over fixed cabling/fibre when serving the on-board maritime commands elements, but may be carried over wireless technology in the event the naval platform is temporarily hosting a land command element and thus supporting its connection to PCore. In this scenario the interconnection to Nation 1's infrastructure PCS, and serviced CC-es, will be provided via a satellite link which carries the PCN-1 interface.

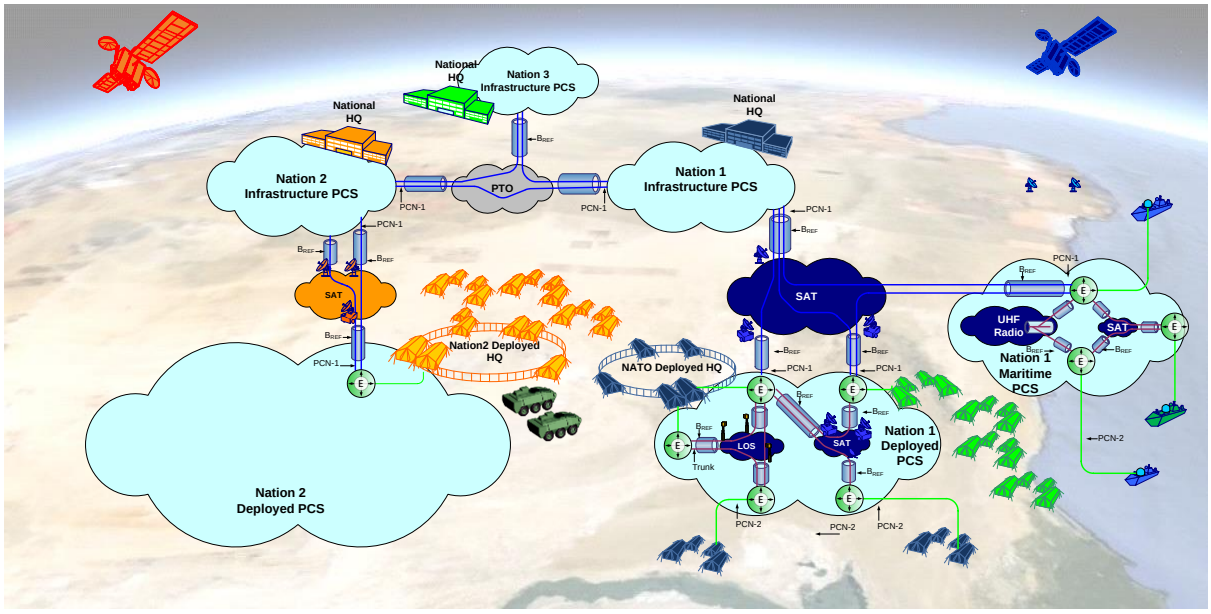

Figure 3: Deployment Phase

1.7.7. Figure 3 shows a snap-shot in time representing the mid-way point of the deployment phase. Nation 1 has already deployed all its ground forces, established its key bases and spreading its forces across its Area of Responsibility (AoR). Satellite links and LOS are used to communicate between E-nodes across the battlefield and further satellite links are used to carry PCN-1 interfaces to the Nation 1's maritime and infrastructure PCS-es. PCN-2 interfaces connect Brigade and Battalion level elements to local E-nodes, normally via fixed cable/fibre. The logical Brigade HQ operational node, which contains physically remote command and logistic elements, has PCN-2 interfaces for CC-es at two different E-node locations separated by a LOS capability as the bearer.

1.7.8. The three PCS-es of Nation 1 together form a PCC. In this way, Nation 1 (as well as other CC groupings connected to these three PCS-es) can always guarantee

that the level of QoS provided by the transport suits the higher level purpose (resources permitting).

1.7.9. Nation 3, like Nation 1, transports its ground forces by sea. However, as it plays more of a support role that a leadership role in the mission its overall land command element will remain at sea throughout the mission. Consequently, it takes advantage of Nation 1's Maritime PCS and connects its CC-es via a PCN-2 carried over LOS. At this point in the deployment, all Nation 3's ground forces have disembarked and are connected to Nation 1's Deployed PCS. Entirely through Nation 1's infrastructure, Nation 3 is still capable of communicating between the CC-es hosting the land command component on a nearby naval platform and the CC-es hosting the forces on the ground. The mobility of PCN allows these same ground forces to find themselves attached to Nation 2 during the engagement phase.

1.7.10. Meanwhile, Nation 2 has begun its airborne deployment. An airfield has been secured which will be used as the logistics store and the temporary command centre for the Brigade HQ. All ground forces have been assembled at the airfield ready for further deployment and an E-node providing reach-back via a satellite carried PCN-1 interface has been established.

1.7.11. Similar to Nation 1, the combination of the Nation 2's Infrastructure and Deployed PCS-es represents a PCC.

1.7.12. The engagement phase (Figure 4) illustrates the situation once all units have taken their respective positions across the battlefield. As Nation 2 is operating in a less hostile environment, trunking between command units (and their associated E-nodes) can be provided by a PTO as well as more traditional military satellite and LOS capabilities.

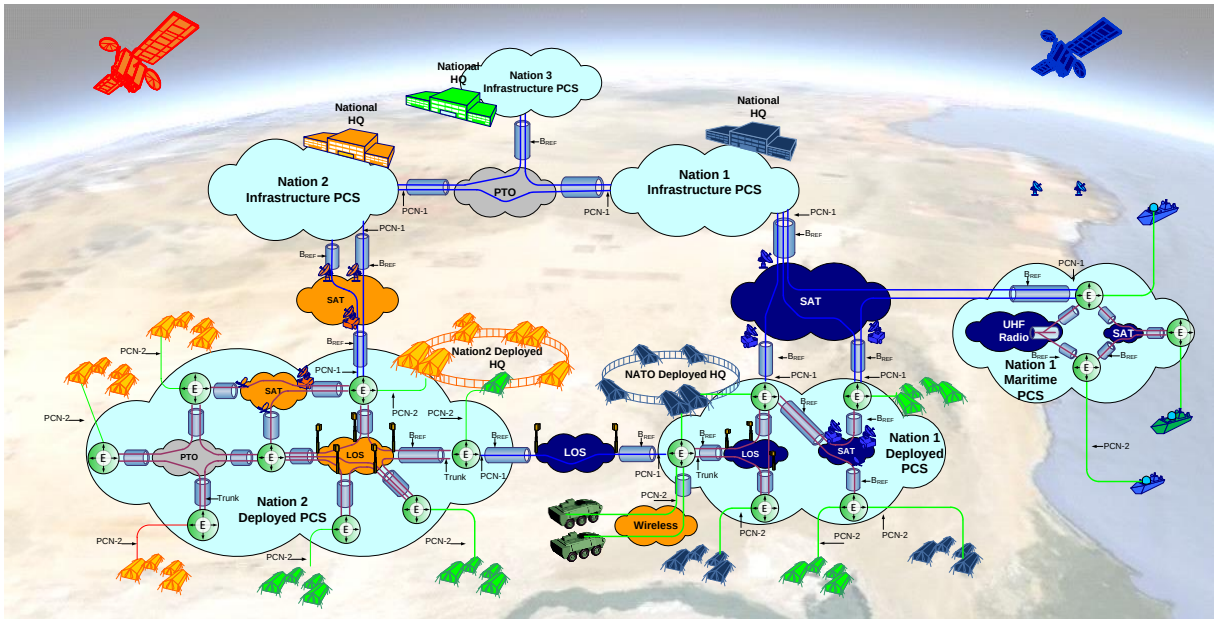

Figure 4: Engagement Phase

1.7.13. Nation 1 takes the responsibility to establish a dedicated LOS capability in order to carry the PCN-1 interface that delivers interconnectivity between the Deployed PCS-es of both Nation 1 and Nation 2.

1.7.14. The combination of the two Deployed PCS-es and the Maritime PCS represents a PCC, which also represents the networking components within the Mission Network. This ensures any combination of CC-es of the same colour can be guaranteed a suitable level of QoS across the entire Mission Network.

1.7.15. Nation 3 battalion level units are dispersed throughout the AoR of both Nation 1 and Nation 2. In each case they connected to an E-node of the respective Nation's Deployed PCS via a fixed cable/fibre that carries the PCN-2 interface.

1.7.16. A two vehicle reconnaissance unit from Nation 2 temporarily loses direct access to Nation 2's Deployed PCS, but is able to quickly regain to relevant services in remote CC-es via a wireless connection access required COI Services finds the need to connect into.

1.8. FUNCTIONAL REQUIREMENTS

1.8.1. The requirements for the PCN ISpec are all functional requirements that indicate the interface functionality as well as the minimum functionality that needs to be in place in the PCS-es. However, to the best possible extent no technology is mentioned in the functional requirements.

1.8.2. To support the PCN Architecture and principles, the following functional requirements that need to be addressed by PCN are identified:

a. PCN shall be agnostic to the employed version of the IP protocol (e.g. it shall be able to handle both IPv4 as well as IPv6 traffic).

b. PCN and its interfaces shall be agnostic to the communications bearer. However, the bearer capabilities shall be based on well-known standards (e.g. IETF, etc.), and shall provide the expected level of service required by the PCN interface.

c. PCore shall manage the resources allocated to the CC-es and enable a fair sharing of available resources according to SLA provisioning.

d. PCN shall support federated networks that may consist of participants at a different PCN capability levels.

e. PCS-es shall mutually authenticate themselves.

f. PCS-es shall authenticate the CC-es connected to them.

g. PCS-es shall provide authentication capability to the connected CC-es.

h. Access to the PCore shall only be granted to authorised CC-es.

i. Authentication and identification shall be supported by deployed trust authorities infrastructures (like PKI) supporting the whole PCore.

j. PCN entities shall employ trust relationships established by federating authentication and identification infrastructures.

k. The PCore shall be considered as an IP network that does not provide any level of information confidentiality; if needed, confidentiality of the information shall be provided by the CC-es.

l. PCS-es shall ensure the Integrity and Availability of the PCore.

m. The PCore shall ensure the Availability of the Transport Services offered to the connected CC-es.

n. The PCore shall provide Traffic Flow Confidentiality (TFC) capabilities.

o. PCS Network Management shall be implemented, whilst individual components can be managed autonomously.

p. A PCS shall be allocated a PCore unique address pool.

q. A connected CC will use address(es) allocated by the corresponding PCS.

r. The required technical services like time synchronization shall be provided between PCS-es, as well as between PCS-es and CC-es.

s. A minimum set of data properties of links shall be defined, e.g. quantitative properties (link capacity), qualitative properties (noise resistance).

t. A minimum set of data to be collected by PCS-es shall be defined in order to build a common network picture, not limited to the network topology.

u. Sensors shall be deployed to monitor PCS resources and detect suspicious behaviour.

v. The collection of data shall also enable the execution of network and security analysis.

w. E-nodes shall maintain information regarding provisioned active connections from themselves to CC-es and other E-nodes.

x. PCS-es and their interfaces shall be able to forward unicast, multicast and anycast traffic.

y. SLAs shall be negotiated and used between the PCN entities.

z. The CC-es connecting to the PCore need to be provided with the Service Level they need for fulfilment of their mission to the best possible extent regardless of the E-nodes they are connected to.

aa. E-nodes shall enforce the negotiated SLAs (including, but not limited to, QoS, security requirements, etc.).

bb. PCS-es shall support different types of traffic.

cc. Service level reporting for individual SLAs shall be performed.

dd. When a PCN entity is no longer trusted, if it misbehaves, or when it breaks an SLA, then it shall be ejected from the PCore.

1.9. SECURITY SERVICES

1.9.1. The Security Services provided by PCN are the following:

a. Authentication and Access Control. Identification and authentication of PCN entities using an established infrastructure of trust authorities (like Public Key Infrastructure – PKI) will be executed to ensure that traffic entering the network comes from a trusted entity. In addition, per packet authentication and authorization will be applied to ensure that the traffic (packets) can be trusted.

b. Integrity. IP traffic protection implemented on PCN-1 and PCN-2 interfaces by the E-nodes will also guarantee the Integrity of the transmitted packets from node-to-node.

c. Traffic Flow Confidentiality (TFC): TFC is a service intended to conceal the traffic characteristics with the objective to prevent traffic analysis across the bearers on PCN-1, PCN-2 or between E-nodes. TFC is widely supported by various standards (e.g. ITU-T X.800, IETF IPSec, or IEEE 802.1AE - MACsec). In PCN, several levels of Traffic Flow Confidentiality are identified which provide different TFC capabilities (like source/destination addresses concealment, packet size concealment, traffic volume concealment, etc.).

d. Availability. The main purpose of PCN is to ensure availability of a transport service to meet the agreed and required service levels of the CC-es. In terms of security related with availability, PCN will provide resistance

against Denial of Service (DoS) attacks and unwanted traffic[2]. This is achieved by two means. First, as already explained non-authenticated traffic is not allowed to enter the PCore. Secondly, the existence of multiple routes between source/destination pairs, resource management optimisation and automated re-routing of traffic in case of (deliberate or not) congestion increases the availability of the network resources. Enforcement of the SLAs ensures that the agreed traffic rate is not exceeded and hence doesn't have a negative impact on the PCore and CC-es.

e. Automatic Risk Assessment. As PCN is to be applied to networks that may be highly dynamic, in particular in the Deployed domain, risk assessments regarding the network availability will need to be updated as changes occur in real-time. However, these assessments will need to also include risks related with confidentiality and integrity.

1.9.2. PCN does not provide information confidentiality of the transmitted data. This is a responsibility of the CC-es themselves; it is initiated/terminated by the crypto devices inside the CC-es and is normally provided through the use of an IP encryption protocol (e.g. IPSec, NINE, etc.).

1.10. QUALITY OF SERVICES (QoS)

1.10.1. To maintain service continuity and to support different types of traffic under various circumstances (e.g. in case of congestion) without requiring over-capacity, Quality of Services (QoS) support is needed. This will ensure that important traffic is transmitted ahead of less important traffic and that real-time traffic can be supported over the converged network.

1.10.2. QoS capability assures the agreed service levels regarding the QoS requirements (like packet loss, transmission delay, delay jitter, etc.) of each traffic class taking into account the competing demands of the network users. To guarantee QoS requirements in a federated context, clear Service Level Agreements (SLAs) between the involved stakeholders are essential. This drives the need for SLA management.

1.10.3. Many QoS models currently exist and hence it is not intended to develop a separate QoS model for PCN. Instead, in principle PCN shall comply with the QoS Model as reflected in and mandated by STANAG 4711. In case this QoS model is not supported by PCS-es, the 4711 QoS model shall be mapped on the QoS model that is supported by that PCS and this shall be reflected in the respective SLAs.

[2] As Availability can also be affected by unintentional system outages (malfunctioning of links and/or network components) this is not considered a security issue, but a technical one, that will be dealt with by PCN by determining alternative solutions to ensure meeting the required Service Levels.

1.10.4. To address QoS, PCN also enables dynamic resource reservation allocated to flows between CC-es. This mechanism is based on signalling and will enable guaranteed capacity, delay, as well as protection from source to destination for specific flows.

1.11. TRAFFIC HANDLING AND SIGNALLING

1.11.1. PCN shall support both Stateless and Stateful traffic handling and signalling at the PCN-1 and PCN-2 interfaces and at the E-nodes. In order to handle traffic in a correct manner, the PCore needs to be aware of the requirements. This can be performed in a stateless manner, where each packet is marked individually, or in a stateful manner, where the properties are signalled and then remembered by the PCore, while each packet is associated to the corresponding “flow”.

1.11.2. Stateless. With stateless traffic handling, the desired properties of traffic handling are attached to each packet. The PCore will forward the packet based on each individual packet marking. A set of traffic classes are created to represent the most typical requirements, e.g. a traffic class for voice could mean a low tolerance of delay, and a fairly low tolerance on delay variation. Voice traffic would then only need to be marked as such, instead of carrying the full property information. Precedence and traffic flow confidentiality requirements would have to be handled separately, as these are independent of the traffic class.

1.11.3. Stateful. With stateful traffic handling, the signalling of the desired properties is performed in advance, before the initiation of the traffic. The PCore will then respond as needed to the signalling request and commit resources (if available). Following the setup of such a flow, every packet that belongs to the flow is forwarded according to the previously signalled properties, which are stored by the components in the PCore. Stateful signalling allows individual setup of flows, and hence a more assured delivery; it also allows feedback from the PCore with respect to the possible service properties.

1.11.4. As mentioned in the previous section, PCN shall comply with the QoS Model as reflected in and mandated by STANAG 4711. This is the case both for stateless (CL) and stateful (CO) signalling.

1.12. MANAGEMENT SERVICES

1.12.1. Management services provide functionality to manage the resource requirements and service delivery. Specifically, on PCN-1 the management service provides the means for PCS-es to exchange information so as to maintain service delivery across the PCore. Moreover, the management exchange on PCN-1 is designed to support federated management, including information exchanges designed to support situational awareness of the PCore. On the other hand, the

management service between CC-es and the PCore on PCN-2 is primarily related with SLA management, where a CC and the PCS agree on the service provided.

1.12.2. As PCN is based on a federated approach, there is no central authority that manages the entire PCore. Each segment is independently managed. Management may be combined if segments fall under the same authority. However, to reach the PCN capability the individual management systems need to collaborate and cooperate. Therefore, different management capabilities are defined that should exist within each PCN entity.

1.12.3. The capabilities and systems required to address the described PCN management services are the following:

a. Network Management and Cyber Defence (NMCD) capability.

b. External PCN Addressing Authority (PAA).

c. External trust authorities (e.g. PKI).

1.12.4. **Network Management and Cyber Defence (NMCD)**. This is the primary management system for a PCS. The NMCD represents all management functionality that needs to take place in a PCS, including PCS performance management and PCS security management. Cyber Defence is an integral part of the NMCD, including Security Analysis and Decision Support functions that support the Cyber Defence capability. The NMCD capability can be viewed as having four phases, analogous to OODA loop (observe, orient, decide, and act); these phases are Sensing and Fusion, Processing and Analysis, Decision Support, and Defensive Response.

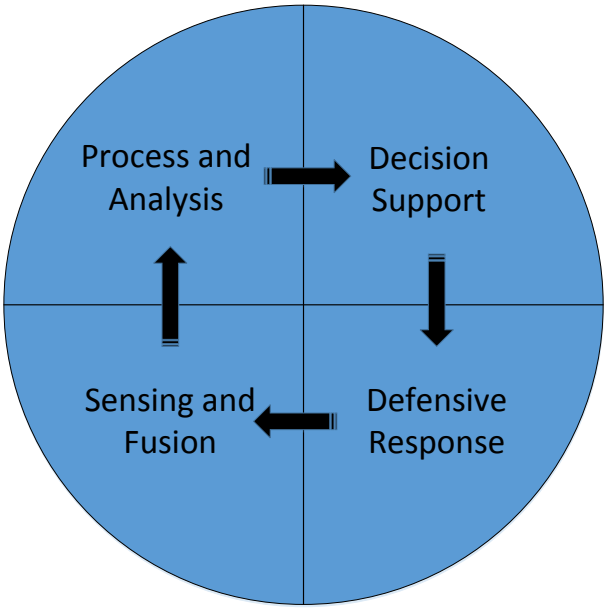

Figure 5: Iterative phases within the NMCD

1.12.4.1. In this cycle, in the Sensing and Fusion phase information is collected from sensors in the PCS and from other PCS-es. The Process and Analysis phase looks at the sensor information trying to identify performance and security issues that need to be addressed. In case of an issue, the Decision Support phase should aid the operator in deciding which action to perform. The selected action will then be executed in the Defensive Response phase. It should be noted that security information from the sensors will be limited to a small number of networks attacks, as per STANAG 5638. Robust network (NIPS, full packet capture) and host monitoring (end-point protection, log collection and correlation from servers, workstations etc.) is out of the scope of PCN and has to be performed at higher layers.

1.12.4.2. The NMCD capability communicates with a number of external components in order to maintain service and security in the PCS. This includes E-nodes, CC-es, internal PCS link providers, as well as other management-relevant entities such as an established infrastructure of trust authorities (like PKI) and the PAA (defined below). In addition, NMCD exchanges information with other NMCD components in other PCS-es in the PCore.

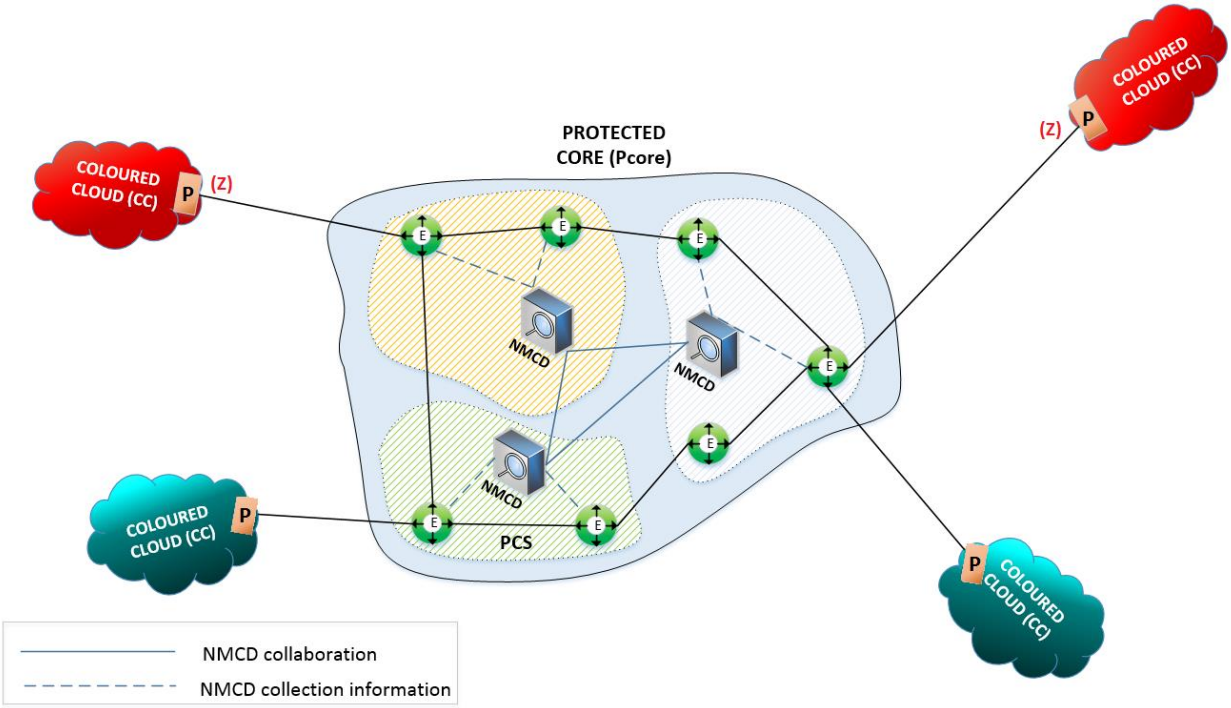

Figure 6: NMCD interactions in PCN

1.12.4.3. The NMCD exchanges the following information:

a. NMCD receives sensor information from the E-node regarding the status, performance, resources, suspicious activity, etc.

b. NMCD controls E-nodes by policy updates and direct commands.

c. NMCD may deploy any number of PCS specific sensors not mandated or specified by the PCN interoperability specification. These sensors will send information to NMCD, and NMCD will control the sensors.

d. NMCD receives sensor information from CC-es, and manages resource requests through SLA management.

e. Internally, a PCS may use multiple 3rd party providers for communications links. NMCD will receive information from these providers regarding status, performance, etc. An SLA stating the expected level of service with these providers should be managed as well.

f. NMCD will interact with multiple trust authority systems when authenticating CC-es and other PCS-es. This involves trust relationships and the update of CRLs or other certificate revocation information.

Suspicion of a private key compromise should be forwarded to the corresponding trust authority.

g. The NMCD will interact with the PAA regarding PCS identification, registration of IANA assigned addresses and PCore/PCN global unicast, multicast and anycast addresses.

h. The NMCD will interact with other NMCDs in other PCS-es with exchange of management information, including resources, suspicious events, and risk related measures.

1.12.4.4. The Management services include SLA Management, Network and Security Management, Security Management and Routing.

a. SLA management includes all functionality for the entities to agree on an SLA, including bandwidth usage, the use of various traffic classes, precedence, as well as TFC. SLA management includes negotiation and re-negotiation of SLAs, as well as change notifications and termination of the SLA. SLA management takes place at PCN-1, PCN-2 as well as between CC-es (referred as an End-to-End SLA). An End-to-End SLA provides end-to-end assurances and/or guarantees for flows between CC-es connected to a same PCC.

b. The security management on PCN-2 (i.e. between a CC and a PCS) includes notifications regarding risk and various security related events.

c. The network and security management on PCN-1 (i.e. between PCS-es) regarding information exchange is much richer and includes various information in support of PCore-wide situational awareness. The exchanged information includes security event notifications, risk level information, cyber defence alerts, network information, and credential management.

d. Routing is only used on PCN-1 as CC-es are assigned addresses by the PCS to which they connect.

1.12.5. **PCN Addressing Authority (PAA)**. When connecting to a PCN, entities such as Protected Core Segments have to provide their own pools of allocated address space. Addresses to PCE-es can be allocated by Internet registries such as IANA, Regional or Local Internet Registries (RIR, LIR). Using global IPv6 addresses would normally prevent address conflicts within PCN. However, as PCN should also be able to cope with IPv4 addresses, a centralized addressing authority is required to avoid

possible IPv4 address conflicts. The PCN Address Authority (PAA) is an administrative function that coordinates, manages and assigns the addresses used within PCN. This includes coordination of used global unicast address ranges, assignment of global anycast and multicast addresses, as well as registration/issue of segment identifiers. There should be only one PAA that manages the addresses for all PCN entities. The allocation process itself is out of scope of this document.

1.12.6. **An Infrastructure of Trust Authorities**. Such an infrastructure (a typical example of which is PKI) is needed for the management of PCN identities. PCN identities are a critical component of PCN as they form the foundation for the trusted overlay created by a PCore. PCN entities use their identities to establish PCN-1, PCN-2, and internal PCS interconnections. Proper management of the PCN identities includes the issue of the certificates, rules for the handling of the associated key pair, and revocation of certificates whose private key has been compromised. As PCN is a federated approach, there cannot be one trust authority that issues certificates to all entities. Rather, there will be multiple trust authorities that issue certificates to different CC-es and PCS-es. In order to allow connections between PCN entities using different trust authorities, a trust relationship amongst them must be established.

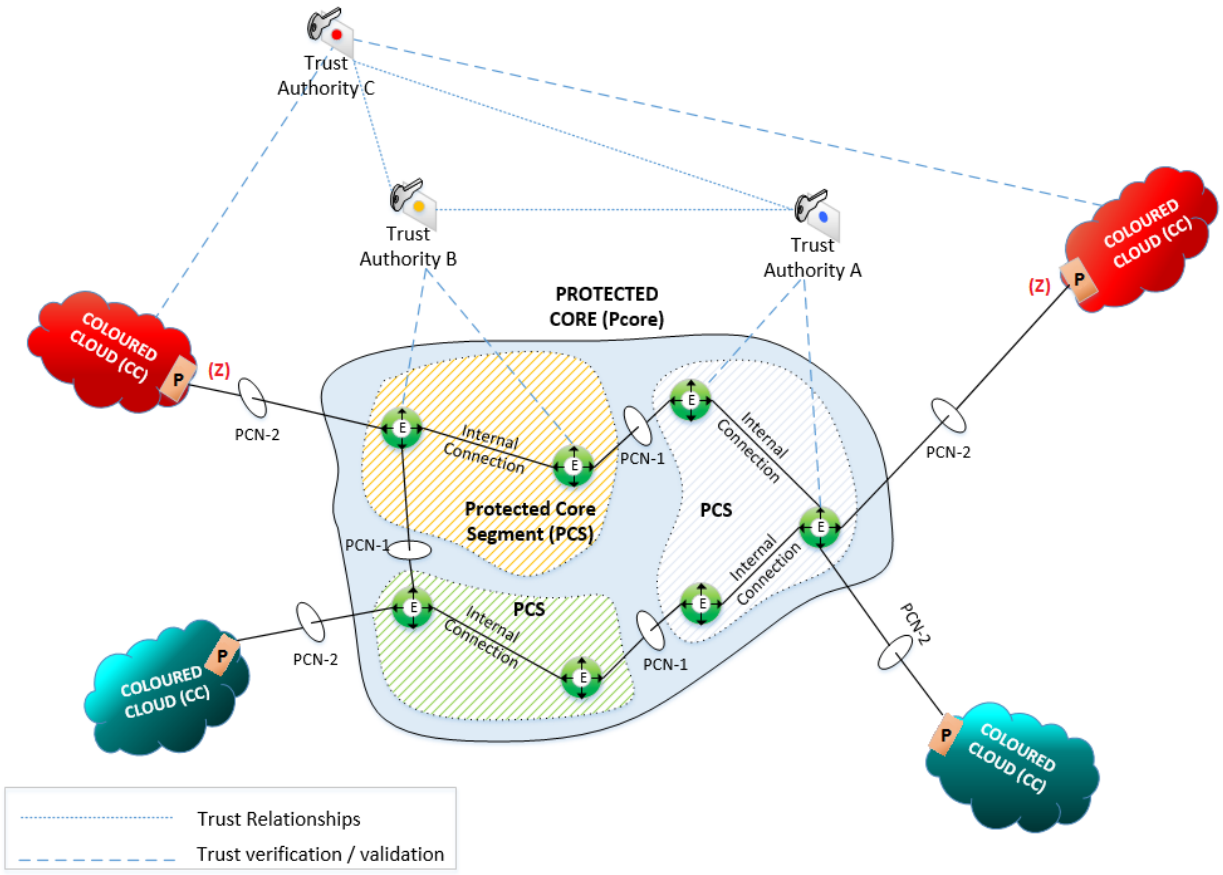

Figure 7: PCN and interaction with Trust Authorities

1.13. CAPABILITY LEVELS

1.13.1. To ensure interoperability between PCN entities with different PCN implementation maturity level (as a result of technological or other constraints), various PCN capability levels are identified [STO AC/323(IST-103)TP/581, 2015]. These are the following:

a. Basic Interoperability: At this level, a nation being in the deployment process to a conflict area is able to leverage the existing PCN infrastructure of another nation for its communications needs following a manual configuration process. This capability allows partners to connect and use the PCore with minimum effort and investment. This is the case when the PCS from nation A provides service to a newly deployed CC from Nation B.

b. Basic Operational Level: At this level, a nation being in the deployment process has replaced manual processes with some automation. This enables basic mobility, with Coloured Clouds being able to disconnect and re-connect automatically.

c. Agility Level: This level enables the automatic exchange of key management information of end-to-end resources. This enables the network to react to physical and cyber threats.

d. Guaranteed Level: This level provides guaranteed end-to-end service based on Service Level Agreements (SLAs) and real-time management of PCS resources. This allows high priority traffic to be prioritized over other traffic, as well as real-time management of the network.

e. Full PCN Level: This level provides fully automated, real-time management including merge and split. The automated risk assessment will enable C2 and J6 Operational Planners to assess the networking risks associated with specific links, areas of operations and connectivity.

1.14. USE-CASES

1.14.1. General. The functional requirements in the PCN Interoperability Specifications (ISpec) need to reflect how PCN should work in a wide variety of situations. To capture the requirements, a number of use-cases or scenarios need to be defined.

1.14.2. Although there are various ways to capture the use-cases, the service-oriented approach is employed. The services supported by PCN are the Connection, the Transport, the Informational and the Management service.

1.14.3. The PCN use-cases will be presented in a new document (to be defined). The existing use-cases from the [RTO AC/323(IST-069)TP/424, 2012] will be used as a baseline but will be modified/adapted to the new Terminology and Concepts as described in this Head STANAG.

1.15. REFERENCES

[RTO AC/323(IST-069)TP/424, 2012]:
NATO Research and Technology Organization Technical Report AC/323(IST-069)TP/424, “Requirements for a Protected Core Networking (PCN) Interoperability Specification (ISpec)”, RTO, July 2012.

[STO AC/323(IST-103)TP/581, 2015]:
Science and Technology Organization Technical Report AC/323(IST-103)TP/581, “Selected Challenges for Protected Core Networking”, STO, April 2015.

[PCN STANAG 5638]:
Protected Core Networking (PCN) Core Specifications – AComP-5638 EDITION A (under development).

[PCN STANAG 5639]:
Protected Core Networking (PCN) Static Specifications – AComP-5639 EDITION A (under development).

[PCN STANAG 5640]:
Protected Core Networking (PCN) Deployable Specifications – AComP-5640 EDITION A (under development).

1.16. ABBREVIATIONS

BCR	Black Core Routing Networks
CIMIC	Civil-Military Co-operation
NMCD	Network Management and Cyber Defence
NEC	Network Enabled Capability
NNEC	Network-Enabled Capability
FoN	Federation of Networks
ISpecs	Interoperability Specifications
PAA	PCN Address Authority
PCC	Protected Core Community

PCN-1	Interface between two PCS
PCN-2	Interface between CC and PCS
PCore	Protected Core
PCS	Protected Core Segment
PTO	Public Telecommunications Operators
QoS	Quality of Service
STANAG	Standardization Agreement
TFC	Traffic Flow Security

INTENTIONALLY BLANK

AComP-5637(A)(1)