Why we believe “Afloat Private Clouds” is a key technology for the future of Digital warships

Christophe BAIXAS[1],
[1] Manager for Scientific and Technical Studies in “Digital Systems”, Naval Group, Ollioules, France

Abstract : The evolution of the navies needs is driving the trend toward collaborative advantage and adaptability while still requesting autonomy, endurance, reliability, cybersecurity, reduced training and standardization. In order to fulfil its missions the warship has to support the massive Data processing and exchange required onboard. To a greater extent than ever before it is essential not only to share IT ressources but also to do it in a way that it makes complexity and flexibility manageable by the crew. Today a new IT infrastructure aboard submarines is rewriting the rules for the way services and functionalities are delivered. Entering “private cloud technology” moves the Combat System from static, inflexible and costly to dynamic, agile and optimized. It allows the resources to be automatically deployed with little or no human involvement. It is a key point for allowing the Combat system to benefit from massive data processing, information sharing, automatization and AI improvements in the next decades.

1 Introduction

Nowadays the Navy’s fleet are facing a broader range of assignments than before. The combat ships of tomorrow will need to be able to cope with new challenges like :

- <u>Broader range of tasks</u> : Deter, Watch / Anticipate, Perform maritime safety and security…
- <u>New warfare capabilities</u> : Drones, Improved weapons, New sensors, Cyber warfare
- <u>New communications and network needs</u> : Shipborne communications, external communications, Interoperable joint forces, Information sharing at a fleet level
- <u>Emerging threats</u> : Cyber attacks, Drones, Anti Access / Area Denial

With this in mind, we can state that tomorrow’s warship will need to be more and more flexible, networked, reliable and secure.

In this regard the usage of IT technology is paramount. Today’s warship is a global information system. It requires data consolidation and information distribution, powerful computing capacities, complex technologies both for combat and platform systems.
The concentration and interpretation of this large amount of information plays an essential role in operational combat decisions.
Further to that, dominance in the information space is considered as a critical capability enabling a navy to determine the way it will engage in sensitive mission or conflict. The one who wants to achieve and maintain its “digital superiority” will have to rapidly and effectively deploy its “up-to-date” solutions onboard.

This kind of capability is not easy to build in a fast changing environment full of legacy systems and obsolescence issues (Hardware and Software). It represents now a major subject in the building of warships.

2 Fast changing expectations

In the last 25 years our world has faced rapidly changing and increasingly complex information and cyberspace environment. Emerging information technology (IT) systems have been developed and implemented faster by the civilian sector than by military industry.
In the higher-threat, information-intensive combat environments of the 21st Century the warships require a more robust, protected, resilient and reliable information infrastructure.
This major transformation is led by strong technical and human trends toward a new “business model” allowing the delivery of extended capabilities. It is supposed to streamline support, training and operating procedures while providing a fully secured access to critical information.

2.1 Technical trends

2.1.2 Stronger usage of COTS

The last decades have seen military users move away from military specified systems to instead exploit the performance, gains and cost efficiencies offered by commercial off-the-shelf (COTS) hardware and software originally developed for the commercial markets.

This migration towards COTS and open systems architecture offers a number of pay-offs : design and development costs can be significantly reduced by avoiding the use of proprietary products and eliminating vendor 'lock-in' at all levels of the system design.

2.1.3 Software technology evolution

Whereas in the past most of the systems architecture were based on hardware solutions nowadays they are more and more built on software solutions. This is of course accompanied by significant increases in complexity. The ways the applications, servers and consoles are working together has evolved from point-to-point, to distributed object, to publish/subscribe, and is now moving toward Service-Oriented Architecture.

During update cycles, the combat system must absorb major requirements and software changes driven by technology evolution in addition to enhancing warfighting capability.

2.1.4 Lower power consumption and reduction of footprint

Today’s warship are more and more “IT oriented” but using legacy technology comes to the limits. Using more servers, gateways and consoles leads to greater power consumption thus limiting the autonomy for the mission.

Increasing the operational efficiency (especially on submarine) is afforded by having low power consumption vessels and ships and smaller systems footprint aboard.

2.1.5 Rise in complexity of IT systems

Combat systems are very large, complex computing systems, consisting of millions of lines of code that must be engineered to meet rigorous mission-critical requirements.

The engineers and navies are more and more concerned about the growing complexity of IT assets and systems and see this trend as a threat to security and stability. The more complex the infrastructure, the more difficult it is to manage, and the more opportunities there are for cyberattacks to breach the perimeter of the combat and platform systems.

2.2 Human trends

2.2.1 Generation Z crew members is coming !

In this age of Internet and communication one of the biggest challenge relates to the coming of generation Z crew members. These high-tech “Internet natives” bring a new set of behaviors, expectations, and preferences.

It adds a layer of urgency and complexity to the way systems and softwares have to be delivered. Tomorrow requires a modern workplace for a modern workforce expressing strong requests :

- **Stop talking about transformation. Get it done**. Gen Z want new digital technologies and automated solutions in place.
- **Think real time. All the time.** Gen Zs won’t wait the traditional days, weeks, months, quarters, or years for feedback, insights, and results. They expect AI and data analytic solutions to be in place in real time to support operational effectiveness.
- **Embrace human–machine interaction.** Gen Zs are OK with interacting with machines, but not by simply pulling a lever or pressing a button. New forms of workplace interaction (from chatbots to augmented, virtual, and mixed reality) need to be addressed.
- **Keep it short, simple, and to the point.** Gen Z workers expect workplace technology to be intuitive, accessible, and easy to use. Out-of-date or difficult-to-use software equals being left behind and may frustrate them leading them to quit the job.

2.2.2 Make it simple !

Even though the IT world has proved to be more and more efficient and complex it has never been so simple for an average user to use its services.

In the combat and platform systems the capacities will evolve over the time but the user experience should always be straightforward and intuitive after a (short) period of training. Everyone using IT systems expect them to allow customization in order for the machine to adapt to human habits or needs.

Fully dedicated to warfighting, the crew members should not have to struggle with integration, connectivity or compatibility issues while using their systems. Accessing the onboard network must be easy, and all the information and application resources that are necessary for personnel to do their jobs must be readily available almost wherever they are. The IT architecture must deliver that functionality without the burden of complex and time consuming re-configuration processes.

2.2.3 Trust the system !

Combat and Platform systems are very reluctant to instability risks (for obvious security reasons). However, the rate of change in computing technologies far exceeds the development and deployment timelines for the combat systems that employ them.

Navies are expecting from IT systems to be able to take over any problem providing always continuity and top performance (especially in combat situation). This is not only a technical problem since it has to deal with the crewmembers mindset.

A system trusted by a user, is one that the user feels safe to use, and trusts to do tasks without fearing harmful, unexpected or unauthorized actions.

Saying that, the rise of IT systems (and the complexity that comes with it) leads to a drawback : how can the crew really trust all these new technologies and rely on its effectiveness ?

2.2.4 Assist Crew Members in managing complex IT systems

Managing the complexity of a submarine is a difficult task. Considering that we can only rely on a very limited number of crew members nobody can expect to have a strong team of engineers and IT specialists aboard.

Due to the rate of change of underlying technology, in order to manage servers, networks, storage, Cyber systems and softwares, the operator has to consult a half dozen tools or more to get raw data, and then struggle to merge the data into something sensible. It's becoming more difficult to provide the level of service, of security, of performance that is required for the IT systems onboard.

Using purely human intelligence makes it almost impossible especially if the mission is very demanding and puts you under stress conditions. It is mandatory for IT systems to allow crew members to manage the interconnections and interactions among IT systems in a way that fits perfectly the combat and platform systems expectations.

2.3 COTS and Open Architecture… Not enough to cope with coming needs

The application of COTS technology, open systems architectures and new business practices have helped in realising major improvements in systems integration over the last 15 years. The navies have upgraded the capabilities of existing warships at much less cost than the previous closed architecture approach.

However the stovepipe engineering where each system builds its own architecture (with specific hardware and software) and benefits of a common “IP network backbone” is by no means the environment which will allow the navies to evolve efficiently over time in a very demanding IT world.

Using Open architecture, COTS and modularity doesn’t by itself guarantee efficiency. With the exponential increase in data use that has accompanied military‘s transition into the digital 21st century, it is becoming more and more difficult for organizations to keep all of their vital information, programs, and systems up and running on legacy systems architectures.

The IT solutions aboard are expected to provide answers to all kind of expectations :

- *Cost Savings* (in obsolescence management, maintenance, exploitation and new capacity integration)
- *Security* (Information Assurance and Cyber threat protection)
- *Flexibility* (ability to scale up the resources depending on operational and functional needs over the time)
- *Mobility* (Gen Z crew members are expecting access to mobile apps not restricted by which device they have got to hand)
- *Insight* (the old adage “knowledge is power” has taken on the modern and accurate form : “Data is the new “black gold”. Data analytics will fuel the future of military readiness.)
- *Increased Collaboration* (Team members can view and share information easily and securely across the IT Infrastructure)
- *Quality in Configuration Management* (managing configurations in silos can lead to users accidentally saving inappropriate versions, which leads to confusion and security issues).
- *Disaster Recovery* (downtime in critical systems or applications leads to operational issues ; the IT solution is supposed to help speed recovery)
- *Loss Prevention* (systems are at risk of losing all the information saved locally ; critical data has to remain safe and easily accessible whatever happens)
- *Automatic Software Updates* (applications should be able to automatically refresh and update themselves quickly and accurately especially if it is to fix security holes)
- *Obsolescence management* (Traditional in-service support obliges to buy large stocks of components and spares, which carries significant up-front costs. Changing the hardware and software in a system shouldn’t mean rebuilding the whole architecture from scratch)
- Sustainability (powering services rather than physical products and hardware and improving energy efficiency)

Agile, resilient, transparent, seamless and secure IT infrastructure and services are requested to transform data into actionable information and ensure mission execution in spite of the persistent cybersecurity threat.
The IT solutions must be adaptive, innovative and capable of seamlessly employing its capabilities across multiple systems, ships, fleet.

3 Complexity puts us to the limits

The computing environment on most naval ships consists of multiple networks, numerous varieties of hardware and a range of software — much of it subject to old and out of date technologies.

Building a Combat System used to be focused on the development and evolution of individual systems, their requirements were based on assessments of gaps in user capabilities that require integration across individual systems to be enabled.
When a system was bounded with relatively static, well-understood requirements, the classical methods were applicable and powerful. But now that the systems are

networked and each is individually reacting to technology and mission changes, the environment for any given system becomes essentially unpredictable.

Addressing the problem only by using latest up to date hardware/software is not enough to handle the critical innovation impact due to the increasing challenges of digital information exchange across "expanding" systems.

The higher the number of technical parts and people involved the more likely a system is to be complex. Complexity is necessary to deal with the uncertainty involved in difficult to solve problems. *It arises primarily from design strategies intended to create robustness to uncertainty in their environments and component parts* (Alderson and Doyle[i]).
Engineers often assume that increasing simplicity leads to increasing robustness - but this is not true. Instead, increasing complexity increases robustness until the solution moves beyond the peak on the robustness curve mainly because of uncertainty (Figure 1).

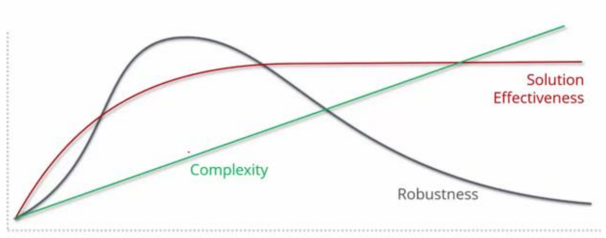

Figure 1 : Complexity, Robustness and Solution Effectiveness.

In this context as complexity is rising, the robustness of the whole "system of system" may decrease after having reached an optimum.
It enters then the "domain of the fragile" (Figure 2) with a major drawback: the solution effectiveness is no more improving and the costs are rising to the top to fix the fragility and complexity issues.

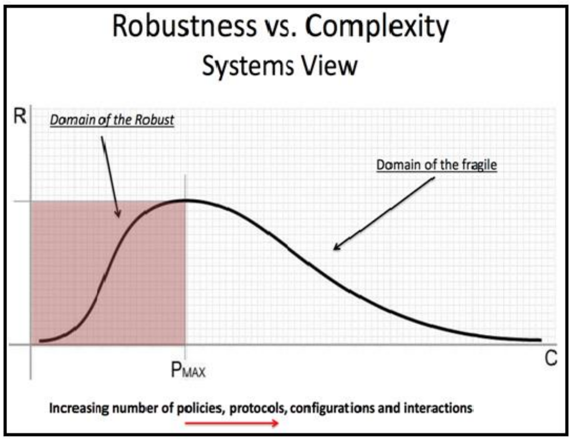

Figure 2: Domain of the Robust, Domain of the Fragile.

The result of stovepiped systems architecture in legacy "SoS architecture scheme" is a slow, disparate information technology infrastructure requiring frequent maintenance, with cyber security bolted on as an afterthought.

4 Cloud Technology : the beginning of the solution

By maximizing commonality the engineers have worked on new architectures making networks easier to operate, creating a common computing environment, reducing costs associated with maintaining legacy systems, and allowing for rapid upgrades.

Once again the solution has been pushed by the civilian world. Enterprises were in the urge to get their applications up and running faster, with improved manageability and less maintenance. It was a matter of enabling IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand, providing the burst computing capability at certain periods of peak demand.

Cloud computing has become integral to modernizing the IT environment and enabling the digital transformation of companies large and small.
It is a method of providing a set of shared computing resources that includes applications, computing, storage, networking, development, and deployment platforms as well as business processes. It is a broad movement to treat IT services as a commodity with the ability to dynamically increase or decrease capacity to match usage needs.

Cloud computing turns traditional siloed computing assets into shared pools of resources that are based on an underlying Internet foundation. It allows users to control the computing services they access, while sharing the investment in the underlying IT resources among consumers. This has helped leading companies lower their operating costs and build modern IT environments capable of rapid, integrated, and highly automated development and operations.
Over the years moving large organizations (with complex IT architectures) applications and data to cloud platforms has involved working through a formidable set of technology, security, operational, and financial issues.

Almost every branch of the economy is today using Cloud Technology from banking to health organizations and GAFAs. That means that the reluctance based on security and stability concern is no more a limited uptake of cloud platforms.

In addition, although various types of attacks can be perpetrated against cloud deployments, they can often be mitigated with proper controls, like with intrusion detection and prevention systems, encryption, and proper configuration. The issue around security isn't only about the technology, it's about operators' ability to configure the tools and build efficient strategies.

Thanks to the wide usage of cloud infrastructure worldwide the technology is evolving at a rapid pace. Major IT solutions providers continue to develop and launch disruptive technologies such as network virtualization, virtual storage, security systems and end-user computing and mobility solutions.

That being said, one could think that using “cloud based technology” on warships is just a matter of adapting “what is working” in the civilian world. Unfortunately this simple answer is not enough to handle the navies needs with the lowest risk, cost and complexity.

5 Building afloat private cloud : the real challenge coming

5.1 “Lift and shift” is not enough

Cloud services provided by Information Technology Partners appeal to many organizations because of their customer portfolio and experience in IT transformation.
But building and managing an infrastructure for a combat system or platform system means dealing with new constraints and requirements that very few are capable of handling in the proper way.
It takes a very good knowledge in submarine and surface warship integration to be able to tailor an IT infrastructure dedicated to naval defence. For Naval Group this experience has been built over the last 30 years after the systems aboard have moved from using dedicated networks to shared IP backbones and now global System of Systems.

Now the defence naval industry runs into two major issues when moving to the cloud :

- The existing applications were created using the traditional IT paradigm. As a result, these applications are typically monolithic and configured for fixed/static capacity. Simply moving them to the cloud will not magically endow them with all the dynamic features of the cloud.
- The typical technology workforce is well versed in developing applications in the traditional IT framework. Most of it will need to be reskilled or upskilled for the cloud environment.

Large-scale move to the cloud isn’t a matter of merely “lifting and shifting” applications and data from legacy systems to cloud platforms. It isn’t a one-size-fits-all IT world anymore. It’s a complex endeavour that requires the naval industry to build new capabilities based on its expertise and experience.

5.2 A technical challenge

Fully embracing the cloud for afloat IT infrastructures requires up-front investments in what is a multiyear journey.
Specifically, there are key topics that should be addressed for successful cloud adoption

5.2.1 Decide on sourcing

It is difficult for any defence industry to build its own cloud-technology stack and even harder to maintain it. Partnering with cloud technology providers (for both hardware and software parts) to build and manage the cloud stack is strongly suggested.
In an effort to continually adapt the latest technologies the pragmatic way is to start by adopting the necessary guiding principles to avoid being locked into one provider.

5.2.2 Create a cloud operating model

Unlike traditional systems operating models using mainly separate equipment linked together the cloud technology relies mainly on abstraction and virtualization. IT infrastructure is managed as code. This requires software engineers familiar with compute, storage, and security protocols adapted to the cloud.
This translates to a massive upskilling of the naval industry in charge of infrastructure architecture and the operating model in which it works. Specific teams need to be assigned to configure and manage this new production environment.

5.2.3 Remediate legacy applications

The transformation of complex systems toward “private cloud technology” is not going to happen in a snapchat.
There will still be legacy applications and systems existing over the time but it is supposed to migrate progressively into the new IT infrastructure model. This is done by following a strategy shared among all the sub-systems.

Existing applications will need to be refactored at the infrastructure and application layers to align with the security and capacity requirements of the cloud. Security must be baked into these applications, and they must work in a more automated fashion. This requires significant attention from application teams, which can be hard to get.

5.2.4 Cultivate the right skills

Professionals must be able to develop applications on the cloud (specifically on the vendor’s system) securely and quickly. To do this, the industry will need to hire and train cloud experts and then introduce them into development teams, retrain or upskill the existing workforce, and set up digital innovation labs as needed, with an emphasis on cloud development.

5.2.5 Securing the Naval oriented private cloud is not like securing “legacy systems”

Developing a cloud-centric cybersecurity model disrupts traditional models and requirements that many navies and industrials have built up over years. A navy making use of private cloud infrastructure needs to evolve its

cybersecurity practices dramatically in order to consume cloud services in a way that enables them both to protect critical data and to exploit fully the speed and agility that these services provide.
This can be a major issue. Despite the benefits of cloud platforms, persistent concerns about cybersecurity for the cloud have deterred organizations from accelerating the migration of their workloads to the cloud.

Developing a cloud centric cybersecurity model requires the systems to make choices about how to manage their perimeter in the cloud and how much they will re-architect applications in a way that aligns with their risk tolerance, existing application architecture, resources available, and overall cloud strategy.

5.2.6 Bringing private cloud in a Submarine... still quite a challenge !

Bringing naval private cloud in a submarine doesn't only mean to provide COTS compliant enclosures. It is also a matter of ship design allowing the integration of shelters or specific IT rooms. These facilities aboard are designed to meet COTS electronic standards, thus saving the cost of developing militarized systems, component-by-component, for shock and vibration. It is also a critical must-have for any ship that wants to manage obsolescence issues in its deployed systems.
Allowing more frequent update cycles will help absorb major requirements and software changes driven by technology evolution in addition to enhancing warfighting capability. The maintenance must be easy and affordable allowing quick replacement and use of hot-swappable components.

5.3 System Enginnering : Entering "Enterprise System Engineering"

The classical systems engineering approach is tailored to and works best in situations in which all relevant systems factors are largely under control by the systems engineering organization or the program manager. The traditional linear process used to develop complex systems is document-intensive and stove-piped leading to very long development times for systems that are cumbersome to change and to sustain.

But now the information revolution increases interactions among people, systems, equipments and it makes everything harder to predict and control.
Today's challenge is to provide design, delivery and sustainment of complex systems in rapidly changing operational and threat environment. Tight budgets and aggressive schedules make it even more difficult to fulfil.
New forms of systems engineering are emerging to address the engineering challenges of system-of-systems (SoS) driven by and deriving largely from advances in Information Technology (IT). This is referred to "Enterprise System Engineering" as it concentrates on managing uncertainty and interdependances in an enterprise-alike environment (*enterprise* refers also in the computer industry to any large organization that uses computers). It encompasses and balances technical and non technical aspects of the problem and the solution.
Critical areas of focus include information assurance, data strategy, interoperability, application integration, information exchange, networks, and communications services (voice, video, and data). No need to say that it requires the involvement of every system contributing to the Combat or Platform system.

5.4 A strong organizational and business challenge involving navies

This disruptive approach relies first on true commitment from leadership in the form of money, human resources and time. On this regard it is important to align implementation effort across industry, government and academia stakeholders.
Building a new "private cloud afloat infrastructure" is first a cultural transformation. That means changing modelling languages, processes, architecture frameworks but also and foremost develop a shared understanding of concepts and ensure consistency and rigor in implementing cloud oriented architecture across systems activities.

This approach has significant management challenges and is not solely in the hands of the industry. The solutions will be built collectively upon alliances and partnerships to co-create and deploy concepts widely used and accepted. It is intended to facilitate the sharing of information and resources in a "reference IT framework".

5.4 Reluctance to change

In the absence of an imperative to change—either from competitive pressures or changing strategic directions or priorities—that reluctance to change won't be broken down.

Three trends, however, will make a race to the cloud inevitable for ship IT Infrastructures :

- **The assimilation of AI** : Artificial intelligence-based technologies are having a major impact on warfighting capabilities in areas like intelligence, risk management, Information dominance, and service delivery. But without a sufficient quantity and quality of data, AI tools and technologies are pretty much useless. As AI is assimilated into the ship technology stacks, cloud computing will become more inevitable and necessary.

- **Rise of complexity in legacy systems brings more risks :** Using legacy systems to handle the challenge of digitalization will cause additional complexity and won't be effective. This will even lead to more attack surfaces for hackers and the additional likelihood that data will be breached. Just making something work is not the answer in this fast changing world. Using up-to-date solutions designed to handle IT complexity is not an option.

- **IT costs :** The need to rein in IT expenditures will put more pressure on navies to adopt cloud computing. The governments and military forces cannot afford to handle heterogeneous frameworks, systems, ships, forces, not optimal in handling, sharing and processing information. Private cloud technology is intended to decompose large monolithic business and technical designs into manageable, capability oriented frameworks that can integrate innovation more rapidly and lower total ownership costs.

6 Naval Group : Building Afloat Common Computing Evolutive and Secured System (ACCESS)

To deal with the increasing digitalisation of our ships imposed by the latest threats and challenges, Naval Group is developing a flexible, scalable solution capable of dealing with the acceleration of technological cycles. Afloat Common Computing Evolutive and Secured System (ACCESS), developed by Naval Group, consists of regrouping and rationalising ship's IT resources, currently disseminated throughout the ship (network, calculation, storage, etc.) into powerful, rationalised, on-board, scalable, cyber-safe and maintainable computing centers.

Naval Group is developing its new generation digital frigate (medium-size frigate FDI) Belh@rra with embedded Datacenters ready to implement ACCESS technology aboard. It will be the first French frigate designed from the onset to be protected against cyber threats, with common computing solution accommodating a great part of the ship applications. The vessel is a powerful and innovative frigate, designed for facing evolving threats.

The Next Generation SSBN submarine will also benefit from this digital transformation. Through increased computing speed, storage capacity and processing capabilities it will allow incorporation of innovative technologies such as advanced computing, Big Data analytics, Artificial Intelligence, autonomous systems and robotics to improve mission effectiveness.

6.1 This is also a matter of S&T Research

Everywhere we look on the warship, the new information paradigm, leaded by the Moore's Law and other forces that bear upon the digital world, is accelerating the way industries have to build their solutions. The development cycle for products and services grows ever shorter. Software is eating the world by automating and accelerating the digital ecosystems. Even in a very sensitive industry dedicated to defense we can no more stand aside from this staggering pace of change.

Having disruptive vision coming into traditional organizations and state administrations is not an easy game. It is not surprising that new ideas rarely map onto the traditional organization chart. Further to that the best inventions and solutions rarely come from experts but from people who offer a fresh perspective.

The S&T Research department of Naval Group has launched an internal project in order to foster innovation and digital transformation in the organization but also toward our customers. We believe that digital transformation is all about a conversation with them and first of all the sailors. If they see their needs and desires being attended to, they are much more willing to persevere through the experimentations and exploration that often comes with exponential growth. Doing a so called "business" analysis, based on User Experience allows our teams to identify the capabilities required on a digital ship.

We then try to iterate quickly and to build knowledge by maintaining connections between our customers and internal community. When engaged properly the customers are not just flexible with the process but they are excited and demand to be part of it. A data centric approach, entailing rapid feedback and timely progression proves to be the best way to make them partners of the solution. That represents a big change toward the legacy "requirements driven engineering" and has impacts on the way we develop. It requires an understanding of the evolutionary trajectory of the technology and a change in our mindset, our culture and openness to diversity (with reliance on innovation from outside and not only inside).

7 Conclusion

The promised benefits of digital innovations (big data analytics, mobility, IoT, increased automation, cognitive computing…) can only be fully realized with a suitable IT solution.

We strongly believe that a naval defence oriented "Afloat private cloud" provides the necessary modern infrastructure and services to deliver capabilities in alignment with mission requirements in a safe and successful way. This modernization is necessary to improve performance, agility, capability, capacity, and security, while reducing cost and complexity.

With this new approach we can keep pace with the rapid changes in technology, defend the afloat assets and foster warfighting superiority.

Last but not least we are not underestimating the unprecedented challenge of embracing automation and technological innovation, without eroding crew members confidence. IT design is a strategic imperative that drives trust and growth. We know that the human brain is built to control its environment — it's a key motivator that drives everyone. If the crews can operate reliably and predictably they will start to trust the IT systems the way they trust humans. Building the afloat private cloud requires to understand the psychological underpinnings of crew members anxieties and use design to address them.

Even as we advance the development of transparent and efficient IT infrastructure there's still one necessary ingredient for trust that can't be manufactured—time.
This will of course require close cooperation between parties, elaborated requirements and tests in harsh conditions.

Author/Speaker Biographies

Christophe BAIXAS, Telecommunications and IT systems Engineer (1998) has been employed by various world leading operators and equipment providers as technical expert. He joined Naval Group as main IT Infrastructure Architect for SSBN and SSN submarines. After a strong Program experience he has been working in R&D Department of the "Systèmes de Mission et de Combat" Division in order to prepare the future IT Infrastructure called ACCESS (Afloat Common Computing Evolutive and Secured System by Naval Group). His research topics include System Engineering, Private Cloud Architecture and handling of complexity in so called "Enterprise engineering".

He his now part of the "Direction de l'Innovation et des Expertises Techniques" (DIT) of Naval Group as "Manager for Scientific & Technical studies" in the field of "Digital Systems".

[i] David L. Alderson and John C. Doyle, "Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures, » IEEE Transactions on Systems, Man, and Cybernetics 40, no. 4 (July 2010) : 840.