Photo courtesy of Deppadesigns/Shutterstock

Securing military networks

With the White House officially elevating the United States Cyber Command (USCYBERCOM) to a full combatant command, the focus on cybersecurity within the Department of Defense (DOD) has never been higher. However, when it comes to securing military networks, how much of a commercial approach to security is applicable? The basic security design principles ought to be the same, but are there differences between commercial and military networks that affect the approaches to be used? Here, Ray Bernard, President and Principle Consultant of security consulting firm RBCS, Inc., and Paul M. Livingston, Non-executive Director at Accokeek Research and Engineering, Inc., address these questions.

One basic difference between commercial business networks and military networks is that for the military, a more disciplined and structured approach is applied to network design and development, as well as to the interconnections between network nodes. Unlike the private sector, there are specific tiers of networks based upon information classification requirements. Principally, these tiers include Top Secret handled through the DoD's Top-Secret Intranet Joint Worldwide Intelligence Communications System (JWICS); Secret handled through the Defense Information Systems Network's (DISN) Secret Internet Protocol Router Network (SIPRNet); and Unclassified/For Official Use Only handled through DISN's Non-classified Internet Protocol (IP) Router Network (NIPRNet).

Each network has its own classification standards for security, which deal with identification (authentication), authorization, access and logging. These are disjointed networks intended to have very few, controlled interconnections rather than a complex pipeline. Connections are tightly controlled and differ going from higher to lower levels of classification, as well as in the reverse direction. There are specific controls on the technologies and protocols being used within classified networks that consider security and integrity before convenience.

In general, the military uses different networks for its day-to-day operations than it does for command and control and intelligence gathering/storing requirements. Different military networks have different security protocols, but controlling the protocols, message exchanges and how applications interoperate are the key means to maintaining control over the overall network. Military networks have identity management and security-related protocols built-in during design and deployment. All classified networks use high-end military grade encryption.

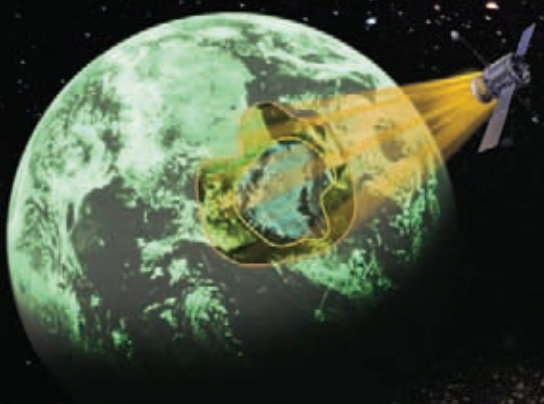
Military networks utilize a very wide variety of technologies. The communications technologies deployed for military air, land and sea operations have operational and security requirements that far surpass most non-military communications operations. In addition, these agencies need to comply with strict security-related oversight including the Federal Information Security Management Act (FISMA) and frameworks such as the National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF).

These aspects of government and military networks make them expensive to deploy and operate; taking smart people to design and run them, and specialized equipment to support them.

Contrasting with commercial networks

In contrast, commercial networks tend to be amalgams due to business growth and changes, including a merger or acquisition, while prioritizing connectivity and data availability (and convenience). Economics and convenience generally drive commercial network decisions. Policy decisions, security, integrity, reliability and purpose drive military network decisions.

In contrast to the government's strict multi-tier network classification scheme, very large businesses often deploy only two-tier networks —one for corporate management and one for business operations. Some highly-regulated businesses, such as utility companies, banks and healthcare organizations have



SMi
LINKING BUSINESS with INFORMATION

SMi's 19th Annual

Global MilSatCom

CONFERENCE & EXHIBITION 2017

Europe's Leading Military Communications Event for Satellite Professionals

Tuesday 7th November - Thursday 9th November 2017 | Park Plaza Riverbank Hotel | London, UK

OPENING ADDRESS:

Harriett Baldwin MP, Minister for Defence Procurement, **UK Ministry of Defence**

HOST NATION ADDRESS:

Air Commodore Nick Hay, Head of Capability C4ISR & SRO for Future Beyond Line of Sight Programme, HQ Joint Forces Command, **UK Ministry of Defence**

KEYNOTE ADDRESSES:

Deanna Ryals, Chief of International MilSatCom, **U.S. Air Force**

Brigadier General Nag Jung Choi, Commander of Defence Communication Command, **Republic of Korea Military***

Colonel Cameron Stoltz, Director Space Requirements, Director-General Space, **Canadian Forces**

Colonel Shinichiro Tsui, Counsellor National Space Secretariat, **Japanese Cabinet Office**

MILITARY AND GOVERNMENT SPEAKERS ALSO INCLUDE:

Colonel Laurent Jannin, Head of Syracuse III and IV Programs and MilSatCom Operations, **DGA France**

Brigadier General Carlos de Salas, Head of C4ISR & Space Programmes, **Spanish Armed Forces**

Colonel Jan der Kinderen, Programme Manager MilSatCom, Defence Material Organisations (DMO), **Netherlands MoD**

Commodore Victor Anuge, Director of ICT, **Nigerian Defence Space Agency**

Lieutenant Colonel Frank Ruckes, Staff Officer, Cyber-/IT- Division, CIT I 3, **German Federal MoD**

Colonel Jorge Vital, Executive Vice President of Space Systems Coordination and Implementation Commission (CCISE), Department of Air & Space Technology - DCTA, **Brazilian Air Force**

Lieutenant Colonel James Dryburgh, DDC4OPS CIS Branch, **New Zealand Defence Force**

Lieutenant Colonel Martin Vlach, Senior Staff Officer, Communication and Information Systems Agency, **Army of the Czech Republic**

Lieutenant Colonel Luigi Mauro, Chief SATCOM Section, Department 1, Computer Science, Telematics and Advanced Technologies, **Italian MoD**

Eron Miller, Chief, SATCOM Division, Infrastructure Directorate, **Defense Information Systems Agency (DISA)**

Major Geoffroy Beaudot, SatCom and CIS Programme Manager, **Luxembourg Directorate of Defence**

Bernd Kremer, Service Line Chief, Directorate Infrastructure Services, **NATO Communication and Information Agency**

Dean Olson, Senior SATCOM Policy Analyst, Chief Information Office, **Department of Defense**

Mike Rupar, Branch Head, Transmission Technology Branch, Code 5550, **US Naval Research Laboratory**

*Subject to Final Confirmation

PRE-CONFERENCE WORKSHOPS | Monday 6th November 2017

A: Global Government Payload Exploration
Hosted by: **The Hosted Payload Alliance**
8.30 - 12.00

B: Interference in SatCom Systems
Hosted by: **Jamie Dronen,** Director, MILSATCOM Future International Programmes, **The Aerospace Corporation**
12.30 - 16.00

LEAD SPONSOR

SES beyond frontiers

GOLD SPONSOR

AIRBUS

SPONSORS

BOEING · eutelsat · GOVSAT · HUGHES · inmarsat · INTELSAT · KRATOS · LOCKHEED MARTIN · Newtec · Raytheon · THALES · UBS · ViaSat

EXHIBITORS

AdvaTech · AEROSPACE · COMTECH · CUBIC · inster · SCISYS · XTAR

To keep updated with programme developments or to reserve your place, please visit:

www.globalmilsatcom.com

Global MilSatCom Community · #GlobalMilSatCom · @SMiGroupDefence

CPD CERTIFIED
The CPD Certification Service

Photo courtesy of sdecoret/Shutterstock

network tiers that confine regulated data to specific networks. The critical infrastructure sector (energy, water/wastewater, transit, etc.) and higher education sector (universities and colleges) may sometimes deploy multi-tier networks – one for business, one for security and one for operations (SCADA) or maintenance. Many commercial organizations typically have a single ubiquitous network with an ill-defined network infrastructure framework, such as the Control Objectives for Information and Related Technologies (COBIT).

Commercial network tiers are not as strictly defined and isolated as military networks, and businesses have more complex mechanisms for identity management layered on top of their networks; in contrast to the more rigorous built-in military approach. Additionally, there is much greater use of high-end encryption in government networks than in commercial networks.

A container approach

One major difference between military and commercial networks is the ability to containerize the information and data residing on military systems. Carnegie Mellon University's Software Engineering Institute developed an approach used to assess an organization's information security needs. Known as OCTAVE Allegro, the method focuses on the information assets on a network. The breakthrough realization underlying OCTAVE Allegro is that security controls are not put directly on the data assets themselves, but on the 'containers' of the data. See Figure 1, which diagrams the OCTAVE Allegro process, in which the container identification step is highlighted.

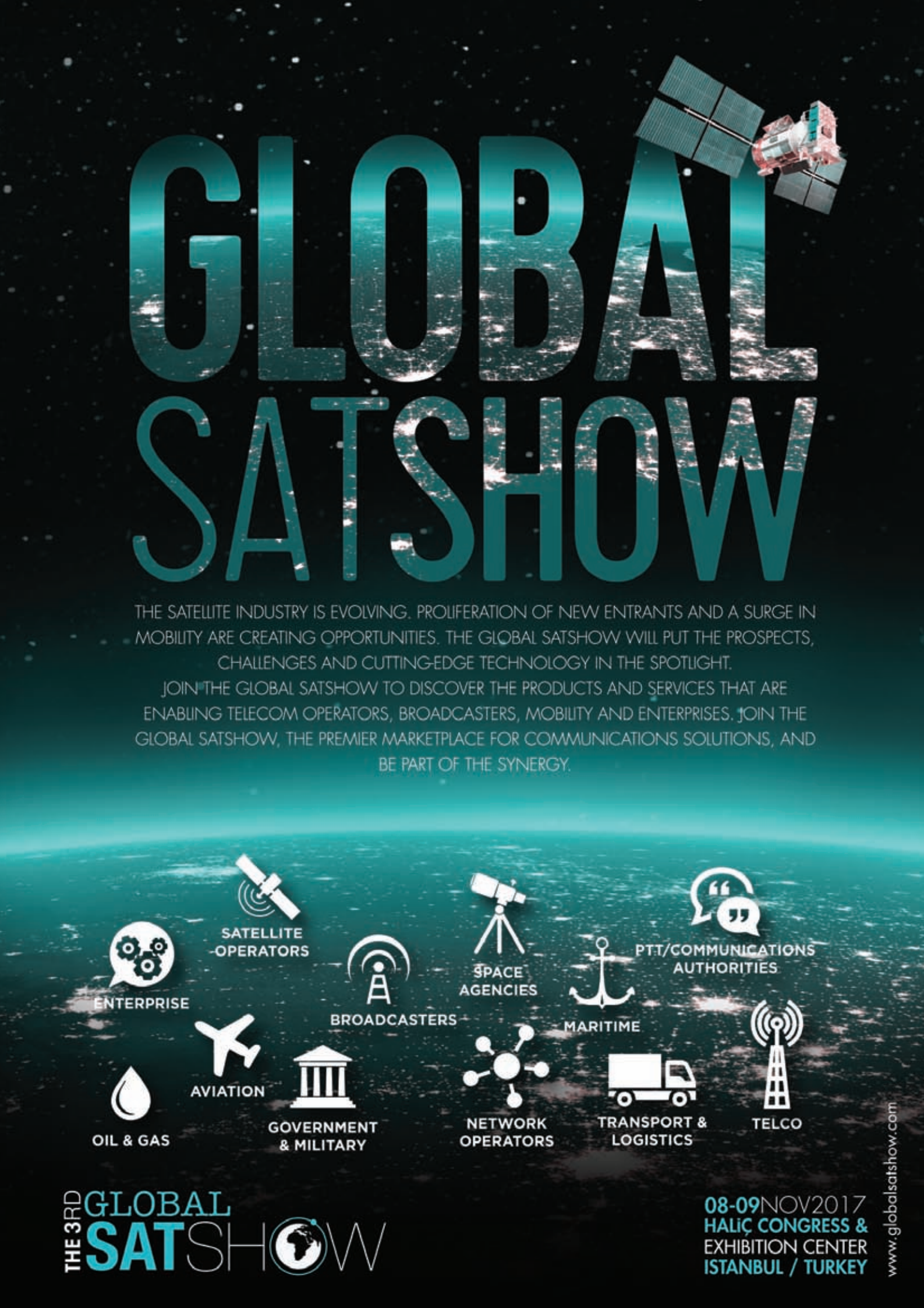
The container approach to information security assessment and planning provides a uniform way to address all three domains of information security: Physical (paper and physical media), electronic (computers, networks and telecommunications), and human memory (where people and process controls apply including responsibility assignments and legal contracts). Due to the highly-structured nature of military networks and their protocols, the network itself can be more easily treated as a 'container' than can be done for commercial networks.

This approach can be more easily applied to military networks to identify important assets and assess them based on the information assets to which they are connected, enabling the DoD to apply security controls directly to those containers.

Thus, the container concept is likely to be very helpful in managing, maintaining and improving cyber security effectiveness while network and communications technologies continue to advance, and are adopted and adapted for government and military use going forward. A consistent approach to cyber security evaluation and planning can be maintained despite underlying networking and communications technology continuing to rapidly change.

Technology trends

The combined effects of several technology trends - such as low power, miniaturization, software-defined networking, system on a chip (SoC), and mesh networking - are leading to network and communications products that have improved mobility, range, and resilience, and are more easily deployable. Consumer product trends now include self-configuring systems with strong certificate-based device authentication and end-to-end military grade encryption. Two key information technology megatrends are the exponential increase in technology capabilities and the exponential decrease in the cost of individual technology components. For example, contrast the cost and capabilities of


GLOBAL
SATSHOW
THE SATELLITE INDUSTRY IS EVOLVING. PROLIFERATION OF NEW ENTRANTS AND A SURGE IN MOBILITY ARE CREATING OPPORTUNITIES. THE GLOBAL SATSHOW WILL PUT THE PROSPECTS, CHALLENGES AND CUTTING-EDGE TECHNOLOGY IN THE SPOTLIGHT.
JOIN THE GLOBAL SATSHOW TO DISCOVER THE PRODUCTS AND SERVICES THAT ARE ENABLING TELECOM OPERATORS, BROADCASTERS, MOBILITY AND ENTERPRISES. JOIN THE GLOBAL SATSHOW, THE PREMIER MARKETPLACE FOR COMMUNICATIONS SOLUTIONS, AND BE PART OF THE SYNERGY.
SATELLITE OPERATORS
ENTERPRISE
BROADCASTERS
SPACE AGENCIES
PT.T/COMMUNICATIONS AUTHORITIES
MARITIME
AVIATION
OIL & GAS
GOVERNMENT & MILITARY
NETWORK OPERATORS
TRANSPORT & LOGISTICS
TELCO
THE 3RD GLOBAL SATSHOW
08-09NOV2017
HALİÇ CONGRESS &
EXHIBITION CENTER
ISTANBUL / TURKEY
www.globalsatshow.com

today's smartphones with the cost and capabilities of the best personal computers available 20 years ago. Many smartphone features were not available then at any cost. Overall, technology is trending in the direction of meeting and addressing many of the challenges faced today in military networking and communications.

Challenges

Carsten Brinkschulte, CEO of Core Network Dynamics, explains: "A key challenge to overcome is that while devices used by military personnel are mobile, the base stations of most current communication systems are stationery, that is they cannot move while in operations. For advanced flexibility and agile deployments, it would become essential to support a mobile network architecture, where the mobile network itself is mobile and can move while providing communication services.

Another key issue is delivering a fully functional, reliable, resilient voice and data communications infrastructure that can be rapidly deployed and works wherever military personnel are, whether operating in built up urban areas or on mobile manoeuvres in remote, resource-constrained environments such as deserts or mountainous areas. It is also important to enable greater network reach, no matter what the terrain, and ensure coverage can be automatically extended as required.

Another significant challenge is to avoid a single point of failure in the network architecture, however existing military communication systems are often relying on a centralized architecture with a single point of failure."

Emerging technologies

Emerging technologies are appearing that have the potential to solve many of the challenges that currently constrain network and communications deployments.

For example, miniaturized, meshed networks, with multi-hop routing based on existing technology standards, could transform mission-critical military communications, once they are adapted for the advanced and special requirements of military use-cases.

By creating small cells which are meshed together, military personnel could be provided a fully functional, miniaturized network wherever they go. Whether operating in built-up urban conurbations or remote areas with patchy or no network coverage, the mobile 'bubble' could move with them. And when such pocket-sized mobile networks are connected to other bubbles using mesh topology, it becomes a network of networks, dynamically extending the reach of the combined network with every bubble added.

A local core network would also be more secure and resilient as it would have no dependency on centralized infrastructure.

Again, such emerging technologies would have to be adapted to incorporate government communications security requirements, such as Type 1 and Type 2 cryptographic security. However, the general direction of technology advancement makes that easier to do with emerging technologies than with older network and communications products.

Conclusion

The differences between military and commercial network security are immense, but the opportunity for the DoD to use a container approach to security is a prime advantage. Given the type and sensitivity of information that is housed on DoD networks, security needs to be one of the top concerns. A properly designed and configured container approach will largely separate container security from underlying transport and access technologies. This approach can help to deliver the required security elements to help deliver on the DOD's national security mission. **GMC**

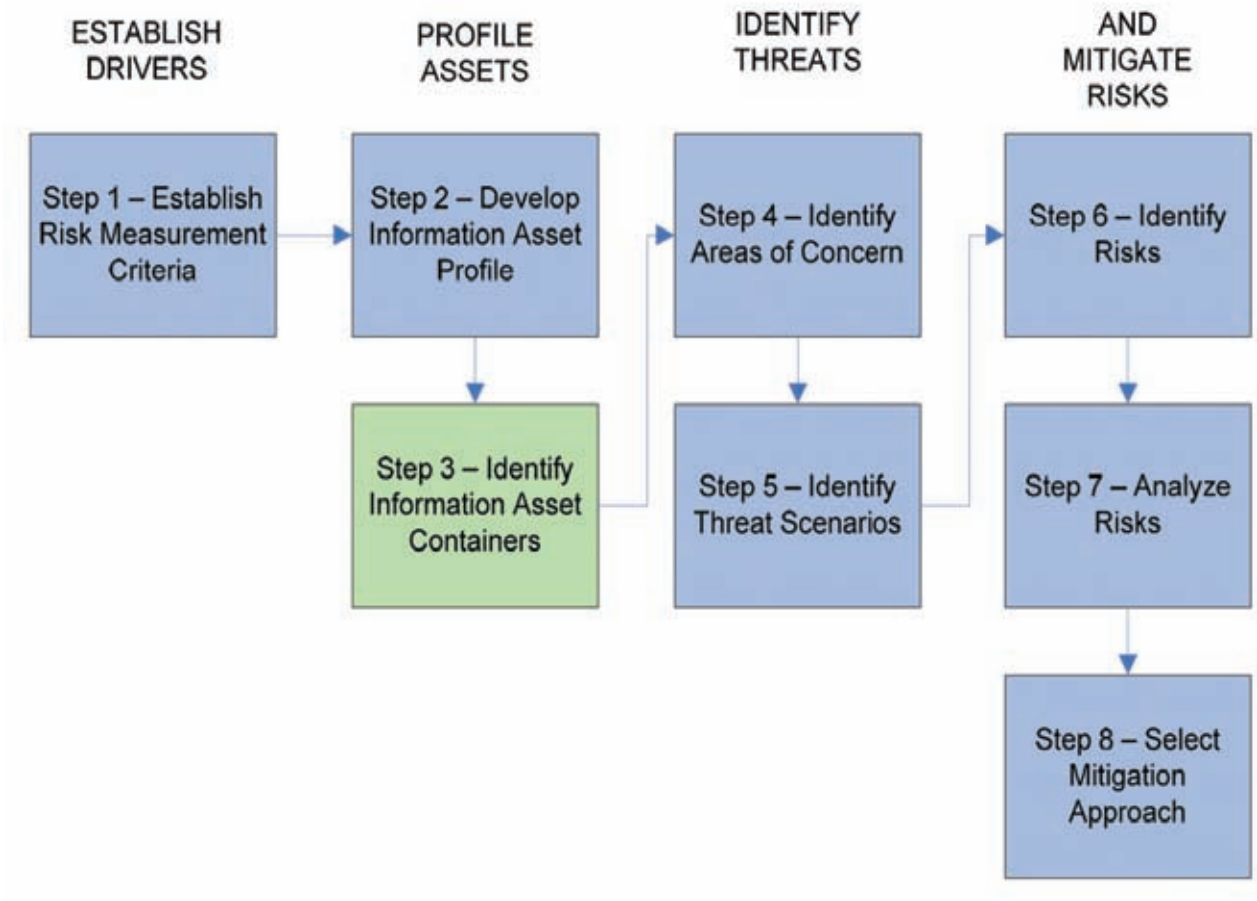


Figure 1. The OCTAVE Allegro process

GVF

Satellite.
Solutions.
The World.

• GVF serves as the unified voice of the international satellite industry •

www.gvf.org