Cyber Symbology

Dr. Margaret Varga
Seetru Ltd., Albion Dockside Works, Bristol, BS1 6UT, UNITED KINGDOM
and
University of Oxford, South Parks Road, Oxford, OX1 3SY,
UNITED KINGDOM
Email: margaret.varga@seetru.com / margaret.varga@zoo.ox.ac.uk

Dr. Carsten Winkelholz and Susan Träber-Burdin
FKIE, Fraunhoferstrasse 20, 53343 Wachtberg,
GERMANY
Email: carsten.winkelholz@fkie.fraunhofer.de and susan.traeber@fkie.fraunhofer.de

ABSTRACT

A symbol is a representation of something such as an object, idea, emotion, relationship or thought etc.; symbols can be composed of words, gestures, sounds, ideas or visual images. Symbols provide an effective mean for people to communicate. In order to use symbols we need to learn the symbols; what they represent and associate the symbols with their meaning. This paper discusses research and development of symbols applied in the cyber domain.

1.0 INTRODUCTION

Symbols and icons provide an effective mean for people to communicate. An icon is a pictorial depiction of the object it represents, i.e. it looks like the object, e.g., a telephone, a bicycle etc. A symbol on the other hand is a representation of an object, idea, emotion, relationship or thought etc. Symbols can be composed of words, gestures, sounds, ideas or visual images. However, in order to use symbols we need to learn the symbols; what they represent and how to associate symbols with their meaning; for example, the chemical symbol for water is H_2O. It can be considered that symbols could be made more intuitive by using pictorial or iconic representations. In general symbols that represent phycial object such as a maginfying glass for search funcion on the computer are easy to construct and establish. However, this is not the case for abstract representation of task, idea, action, thought, application etc.

There are pros and cons in using icons or symbols. Ideally, an icon enables immediate understanding as anyone can tell what it stands for at a glance. This makes the iconic representation intuitive and easy to use. A symbol, on the other hand, can be more complex to understand, but it can also be given very specific meaning, thus having great potential as an information carrier. A set of symbols can be created for specific purposes, domains or applications [15].

We all use symbols, for example, numerals are symbols for numbers, country flags are used to represent countries. Symbols have been developed and used in many different domains and applications, such as the highway codes, maps, computer networks, currencies, chemistry etc. In the computer system, symbols and icons are used to represent tools, applications and commands, such as firewall, router, switches, workstation, search and save functions etc.

A tick mark (√) is a commonly used symbol to mean "yes": such as, "yes", this has been checked or, "yes"; that is the right answer or "yes" this is what I choose. However, sometimes the same symbols can mean different things under different contexts or for different purposes, for example although "x" normally means no, wrong answer, but it is sometimes used to mean yes in the case of election ballot papers. Similarly, Y and N also commonly used to mean “Yes” and “No”.

2.0 CYBER SYMBOLOGY

In military applications; symbols have been designed and used to represent physical objects such as aircraft, tanks, vessels. In the Air, Land, Space, Sea surface and subsurface such symbols are typically displayed on a geospatial map [4 and 14]. The situation in the Cyber domain is not quite so straightforward; although there are physical entities in the Cyber domain, such as workstations, routers and printers, their characteristics are not necessarily of the same nature as the conventional physical objects in the other domains. Cyberspace is recognized as a critical domain of military operations. However, Cyberspace is not an isolated domain; it is omni-present in all of the other domains. For instance, an unmanned aerial vehicle (UAV), also known as a drone, is part of an unmanned aircraft system (UAS) which includes the UAV, a ground-based controller as well as a system of communications between the two. The UAVs can be controlled by a human operator using a remote control or autonomously by computers on-board the UAV [8]. In the Cyber domain the UAV characteristics may include the physical location of the UAV, its mode of operation, its associated ground control station and perhaps a satellite network, it can also include the effectiveness, stability, strength and reliability of its associated communication network. Furthermore, a UAV also has its own internal network for its systems and control, and this may also need to be represented. Similar, but often more complex, illustrations can be built for all the components of Cyber systems. This illustrates some of the complexities and challenges of designing and applying symbology in the cyber domain. In short, representations in Cyberspace need to be radically different from those in physical space, and the manner in which users interpret the symbols and thus become aware of the situation, its effect and impact is also radically different.

Although the need for symbols in Cyberspace has long been recognized, and research and development has been conducted into designing symbol for the cyberspace, there is, as yet, no agreement on how to symbolize entities and activities so that commanders and decision makers can comprehend the impact of the Cyber situation in their mission planning and execution.

DARPA’s Plan X seeks to develop a defensive platform for the Department of Defense (DoD) to conduct and assess cyberwarfare in a manner similar to kinetic warfare. It is concerned with, for example, how to make it easier for humans to visualize a network and its components, to automate the task of identifying anomalies that might appear on that network as benign or hostile, to provide symbology that can present to the users the status of various components of a network intuitively, effectively and efficiently. So as to enable even inexperienced users to take action to prevent hostile parties / attackers from gaining access to and causing damage to components in cyberspace, such as a control system or a network [3].

The effectiveness of a symbol can be measured by how well it communicates the information in its representation and how easily the user can comprehend and exploit it for situation awareness and decision support / making. This is governed by the operational context and its intended purposes, the tasks and the users.

This paper discusses the research and development of symbology in the cyber domains and its challenges.

3.0 CYBER SITUATION AWARENESS

There are many different definitions of situation awareness (SA); Ensley, however, provides an established definition of SA for dynamic environments:

> *Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning and the project of their status in the near future [5]*

Furthermore, for Ensley, situation awareness is a state of knowledge and situation assessment is a process of achieving, acquiring or maintaining situation awareness [5 and 6]. Acute situation awareness can potentially enhance the quality and speed of our decision making process.

4.0 HUMAN FACTORS

Determination of the most effective way to present cyber information greatly depends on the specific user(s) and their goals, objectives, tasks and mental models. Figure 1 shows the US Cyber Command Computer Defense Network – Service Provider (CND-SP): each tier is composed of different types of users with different objectives, needs, and tasks; thus, the symbols required will be different to communicate the different type of information for situation awareness so that appropriate decisions could be made [11].

At Tier 3, for example, the types of users and information required in the Information Assurance / Cyber Network Defense activity would be very different from the Tier 1 Policy and Oversight activities. It is therefore illogical to expect that a single information interface / cyber symbol sets will be able to support effectively all the types of users with their different tasks and needs. Indeed, a human factors design process is vital in supporting the conception, development, and testing of the variety of cyber information interfaces and to determine where it is applicable to include symbology and / or icons as well as their nature and their effectiveness in supporting specific users performing their particular tasks.

The human factors design process begins with Analysis, which is vital to the success of the design process as it provides the foundation to support all subsequent design activities. The Analysis phase provides an essential opportunity for the design team and the end-users to form mutual understanding. The end-users provide the design team with valuable information and insight about the work domain, such as overall objectives of the work, tasks, the sequence and dependencies of the tasks, information required, etc. The design team uses human factors techniques and methods such as interviews and work-flow diagramming to gather information for further analysis, including specific techniques such as goal-directed task analysis [11, 17 and 18]. Information gathering and analysis help the design team to understand the stakeholders and their tasks, the information needed and the decisions to be supported, available sources of information, information and process gaps etc.

The measurement of human performance and situation awareness are governed by an in-depth understanding of the operational environment. The analysis phase enables the deign team to determine what is the best way to support the work processes of the users in a way that facilitates their cognitive and perceptual needs. However, it is challenging to convert the information gathered during the analysis phase into the initial design concepts - which are the integration of the gathered information with the foundational knowledge of human perception and cognition guided by the human factors design principles that have been developed from decades of research in determining the most effective ways to display information for different uses and applications. Once the information from the analysis phase is implemented into an initial design, the design team can begin developing the tool/work-aid interfaces and functionality. The design team also needs to determine what data is required to support the interfaces and visualization, and consider how the data can be accessed effectively as well as the allocations of the tasks. Interaction between the design team and end-users is vital for refining initial designs during the Iterative Design & Testing phases, during which the products are tested, refined and tested again to achieve maximum utility and usability. The evaluation would involve user-in-the-loop testing with operationally representative scenarios and representative user tasks. This would result in fieldable user-centered cognitively sound and usable cyber tools.

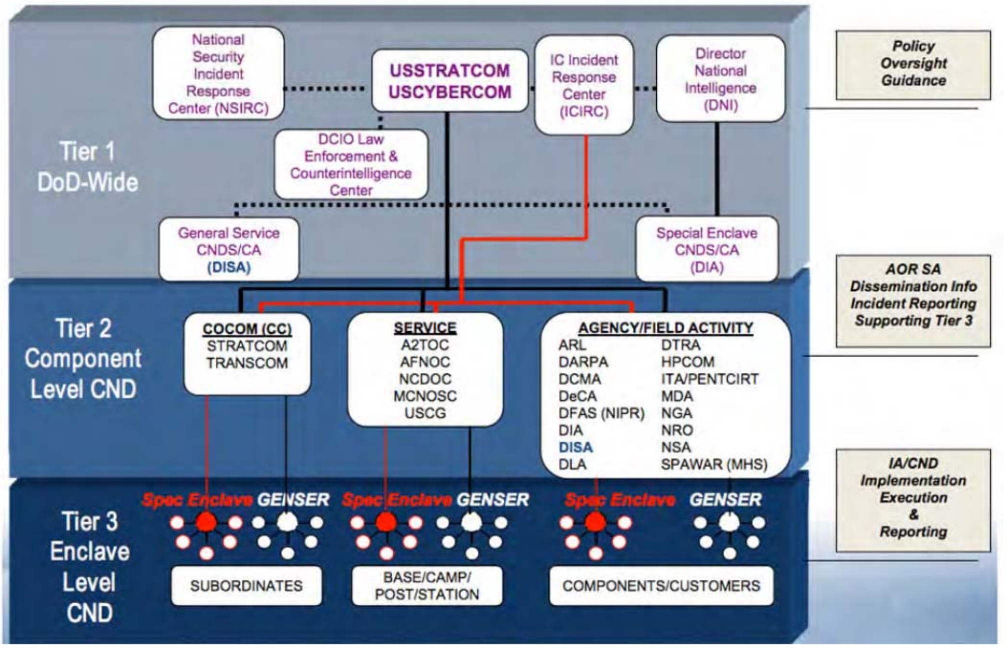
National Security Incident Response Center (NSIRC)
USSTRATCOM
USCYBERCOM
IC Incident Response Center (ICIRC)
Director National Intelligence (DNI)
Policy Oversight Guidance
Tier 1 DoD-Wide
DCIO Law Enforcement & Counterintelligence Center
General Service CNDS/CA (DISA)
Special Enclave CNDS/CA (DIA)
AOR SA Dissemination Info Incident Reporting Supporting Tier 3
Tier 2 Component Level CND
COCOM (CC)
STRATCOM
TRANSCOM
SERVICE
A2TOC
AFNOC
NCDOC
MCNOSC
USCG
AGENCY/FIELD ACTIVITY
ARL
DARPA
DCMA
DeCA
DFAS (NIPR)
DIA
DISA
DLA
DTRA
HPCOM
ITA/PENTCIRT
MDA
NGA
NRO
NSA
SPAWAR (MHS)
IA/CND Implementation Execution & Reporting
Tier 3 Enclave Level CND
Spec Enclave
GENSER
Spec Enclave
GENSER
Spec Enclave
GENSER
SUBORDINATES
BASE/CAMP/ POST/STATION
COMPONENTS/CUSTOMERS

Figure 1: US Cyber Command as the Tier 1 Computer Network Defense - Service Provider (CND-SP) [12]

5.0 CYBERSPACE

Joint Publication 3 12 Cyberspace Operation, describes cyberspace in three interrelated layers namely, physical network, logical network, and cyber-persona, see Figure 2 [9]. Each layer focuses on different aspect of cyber operations that may be planned, conducted, and assessed. The physical network layer is composed of IT devices and infrastructure - the physical domain. It provides services such as transport, storage and processing of information within cyberspace and has characteristics such as geographic location and legal framework. The logical network layer on the other hand is composed of elements of the network related to one another based on the logic programming that connects network components. Individual links and nodes, data, applications, and network processes not sharing a single node are represented in the logical layer. The cyber-persona layer is composed of network or IT user accounts, which can be a real human user or automated, and their characteristics can include their relationships to one another. Cyber-personas may relate directly to an actual person or entity, consisting some personal or organizational data such as e-mail, IP addresses; financial account number or passwords. However, any individual can create and use multiple cyber-personas with multiple identifiers in cyberspace, simples example of this are separate work and personal email addresses or phone numbers.

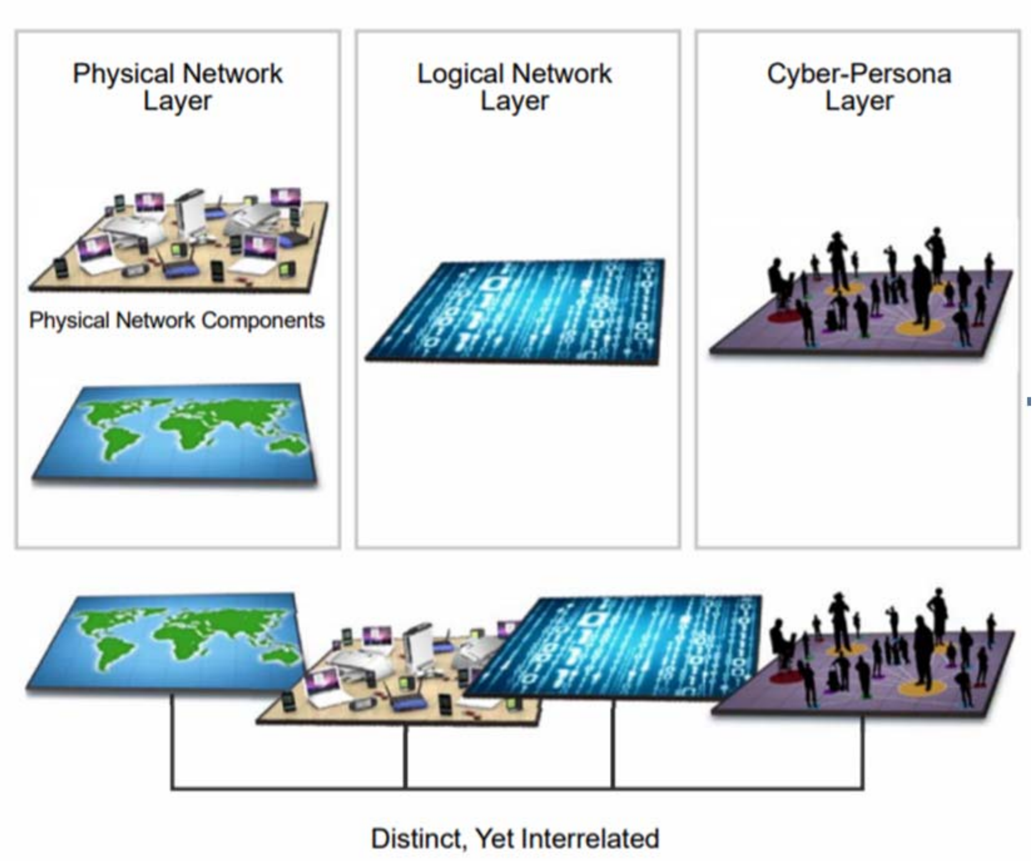

Figure 2: Cyberspace Layers [9]

6.0 MIL-STD-2525D AND APP-6

The Military Standard MIL-STD-2525D is a major document which defines the rules and requirements for the development and display of joint military symbology in the US within the Department of Defense (DoD) and non-DoD entities across all Services and functions. MIL-STD-2525D is concerned with geographic-centric representation of the physical layer and covers an extremely wide range of military symbology applications and requirements. The objective of MIL-STD-2525D is to support interoperability at the information level within the area of joint military symbology. This is achieved by defining a standard set of rules to construct and generate symbols in Command and Control (C2) systems. The rules in this Standard thus ensure that information contained in the joint military symbology can be exchanged successfully across service and organizational boundaries [4].

In June 2014 an initial set of cyber symbols were added to MIL-STD-2525D through the addition of Appendix L [4].

NATO STANAG APP-6 is the joint NATO Standard for Military Symbology for military symbols for maps. It was first published in 1986 as Allied Procedural Publication 6 (APP-6), NATO Military Symbols for Land Based Systems. However, over time the standard has evolved. APP-6D version 1 was published in October 2017. The symbols provide a standard set of common operational symbols that are designed to enhance NATO's interoperability. In joint and combined military operations, it is vital to have a common language that is understood among all users with varying experience and knowledge from different forces, units, organizations or nationalities. Indeed, graphical representation of objects, commands, movements and additional information can be assimilated by users much more readily and effectively than solely text (language) based communication, which can be misunderstood, misinterpreted and imprecise, ambiguous and also slow in transmission [1 and 14].

APP-6 aims to support a standard visual portrayal for all C2 symbols and Control Measures symbols applicable to all NATO nations, coalition of NATO nations, partners, non-NATO nations as well as other organizations. APP-6 is a single system of joint military symbology for land, air, space and sea-based formations and units, which can be used in electronic / automated display systems and manual applications. The symbology takes the form of graphical symbols for visual representation of physical objects, activities or events. Furthermore, the symbols are designed to be applicable in multi-chrome and mono-chrome displays and can be hand drawn easily with pencil and paper. The symbols are overlaid on maps and charts that enable unambiguous and speedy understanding of complex operational environments, i.e. common operational picture (COP). This supports commanders in their assessments of effects, threats and hazard and in their decision making processes. However, the use of many and complex symbols quickly results in cluttered displays and overloaded users, i.e. degrading ease of situation awareness. The use and understanding of the symbols requires training.

APP-6 recognizes the need for Cyberspace in Space, Air, Land Surface and Subsurface domains and work is underway considering the way forward.

The objective of both APP-6 and MIL-STD-2525 is to develop comprehensive joint military symbology that is common to both organizations. MIL-STD-2525D will act as the base document for APP-6(D) as the two documents are migrated to align more closely.

In both cases, a 'building block' approach is used for the military symbols. An icon-based symbol is used to depict units, equipment, installations, activities and meteorological occurrences etc. which are located within and around a virtual bounding octagon concept, see Figure 7. The symbol sets covers the graphic representation of equipment, units, installation and other relevant joint military operations' activities and elements, ranging from, air, land, maritime, space and the display of stability activities and civil support activities. The graphical joint military symbols are used to convey information about the depicted object, which can be a physical (units, equipment), non-physical (planning) or predicted locations with temporarily assigned characteristics or validity. It can be made up of (1) frames, (2) icons, (3) modifiers and (4) amplifier as well as color, graphics and alphanumeric representations that the users can use to construct the required symbol. Each of these elements will be discussed briefly below.

6.1 FRAME

The frame is the border of a symbol and is optionally used in two cases only, i.e. for land equipment and sea surface civilian vessels. Natural event symbols are not framed, i.e. they are 'unframed'. When a frame is included in a symbol, its shape represents the standard identity, dimension and status of the object. A frame can be black or white depending on display background. When the symbol is unfilled, the frame should be displayed using the specified default colours to provide the information about standard identity. Figure 3 shows the frame shapes for real-world, non-exercise situations, different frame shapes are used for exercises, simulations and training.

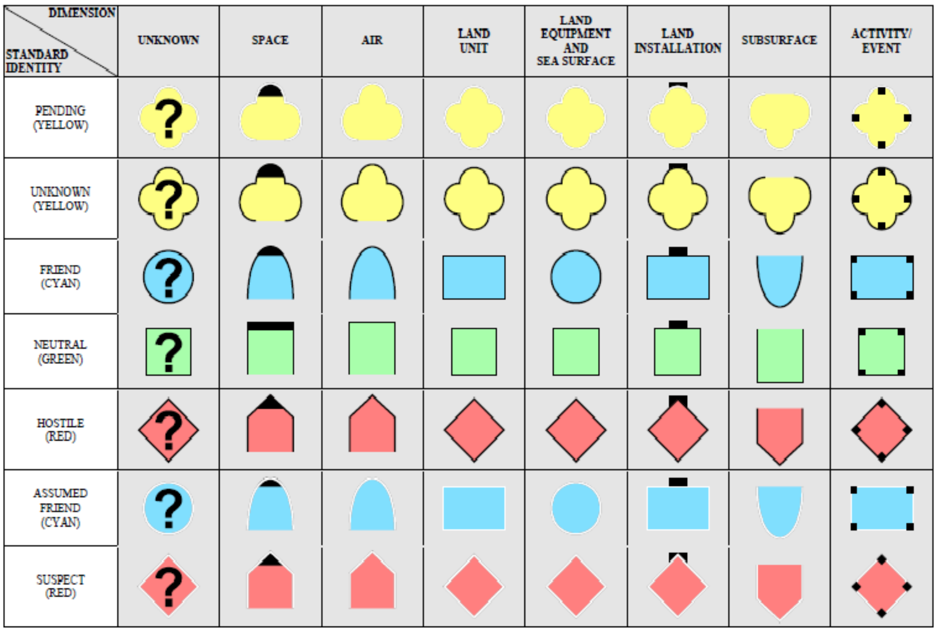

Figure 3: Standard Identities and Dimensions [4]

6.2 STANDARD IDENTITY

There are seven different standard ‘Identities’, namely, pending, unknown, friend, neutral, hostile, assumed friend and suspect. When the frame is closed it represents the Land and Sea Surface Dimensions. Air and Space Dimensions are represented by a frame with open bottom, and an open top frame represents the Sea Subsurface. In the case of Identities such as Friend, Hostile, Neutral and Unknown, a solid frame line is used; whereas a dotted line with alternating black and white dots is used for Identities such as Assumed Friend, Suspect or the Pending Category. Figure 4 shows some example frames for assumed friend, suspect and confirmed neutral in the air domain.

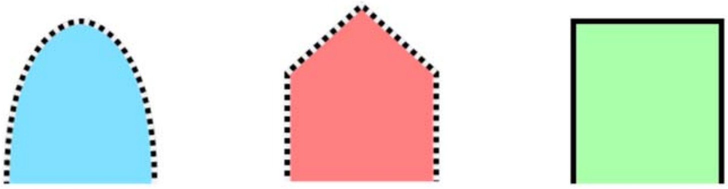

Figure 4: Example assumed friend, suspect and confirmed neutral frames

The term ‘Dimension’ is used to designate the physical environment of the location of the entity or where the primary mission of the object takes place, e.g. Air, Land, Sea etc. An object can have a mission on, above, or below the earth’s surface.

6.3 STATUS

Status reflects the state of the entity’s location or condition which can be Present or Confirmed, Anticipated, Planned or Suspected, see Figure 5. Solid line frames mean that the status is Present or Confirmed. Dash line frames are used to indicate Anticipated, Planned or Suspected status; but, when the

Identity is Assumed Friend, Suspect or Pending the status will not be displayed.

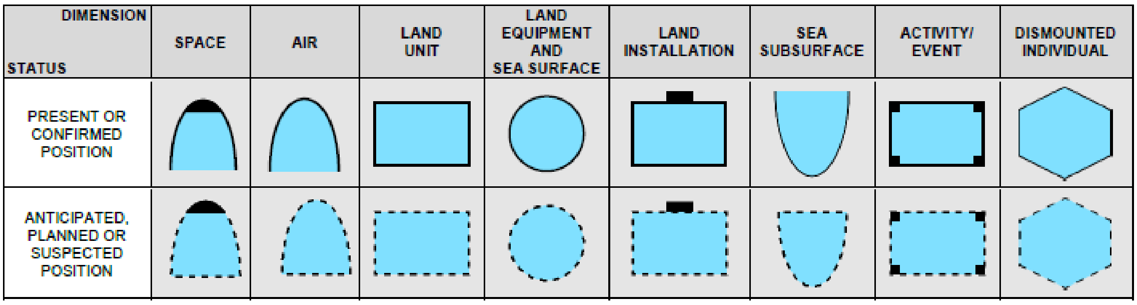
DIMENSION
STATUS
SPACE
AIR
LAND UNIT
LAND EQUIPMENT AND SEA SURFACE
LAND INSTALLATION
SEA SUBSURFACE
ACTIVITY/ EVENT
DISMOUNTED INDIVIDUAL
PRESENT OR CONFIRMED POSITION
ANTICIPATED, PLANNED OR SUSPECTED POSITION

Figure 5: Friend Frames for Present and Planned Status [4]

6.4 FILL

Colour is used to fill the interior area within a frame. Colour is redundant when the symbol is framed so a transparent frame can be used. In the case of unframed symbols colour provides the only indicator of the standard identity. The default colours are used to represent the Standard Identity, Figure 6.

DESCRIPTION	HAND DRAWN	COMPUTER GENERATED		
		DARK	MEDIUM	LIGHT
HOSTILE, SUSPECT, JOKER, FAKER	RED	🟥	🟥	🟥
		RGB (200, 0, 0)	RGB (255, 48, 49)	RGB (255, 128, 128)
		HSL (0, 255, **100**)	HSL (0, 255, **152**)	HSL (0, 255, **192**)
FRIEND, ASSUMED FRIEND	BLUE	🟦	🟦	🟦
		RGB (0, 107, 140)	RGB (0, 168, 220)	RGB (128, 224, 255)
		HSL (138, 255, **70**)	HSL (138, 255, **110**)	HSL (138, 255, **192**)
NEUTRAL	GREEN	🟩	🟩	🟩
		RGB (0, 160, 0)	RGB (0, 226, 0)	RGB (170, 255, 170)
		HSL (85, 255, **80**)	HSL (85, 255, **113**)	HSL (85, 255, **213**)
UNKNOWN, PENDING	YELLOW	🟨	🟨	🟨
		RGB (225, 220, 0)	RGB (255, 255, 0)	RGB (255, 255, 128)
		HSL (42, 255, **110**)	HSL (42, 255, **128**)	HSL (42, 255, **192**)
CIVILIAN (OPTIONAL FILL)	PURPLE	🟪	🟪	🟪
		RGB (80, 0, 80)	RGB (128, 0, 128)	RGB (255, 161, 255)
		HSL (213, 255, **40**)	HSL (213, 255, **64**)	HSL (213, 255, **208**)

Figure 6: Colour range values for filled symbols [4]

6.5 ICONS

The icon is an abstract pictorial or alphanumeric representation of units, equipment, installations, activities or operations and is placed in the centre of the symbol. 'Main' icons are placed in the central main sector of the bounding octagon, see Figure 7. A modifier is an alphanumeric or abstract pictorial representation that is displayed together with an icon. It provides additional information about the icon. Modifiers are placed in the bounding octagon and appear either above, below or beside the icon. Optional additional information about the symbol is provided by an amplifier which is placed outside the Frame, Figure 7.

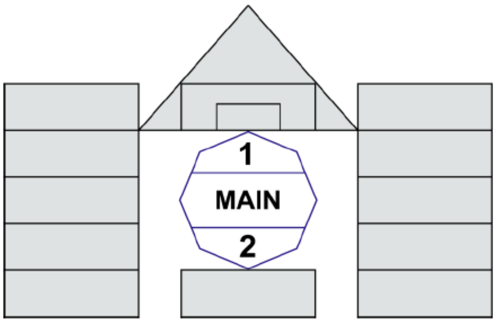

Figure 7: Standard Amplifier Fields [4]

Figure 8 shows an example of an air icon-based symbol. The frame shows that it is a friendly military rotary-wing cargo aircraft with light cargo capacity. The text Amplifiers show the Track Number (TN) 2468 and the priority mode 2 with code 1389.

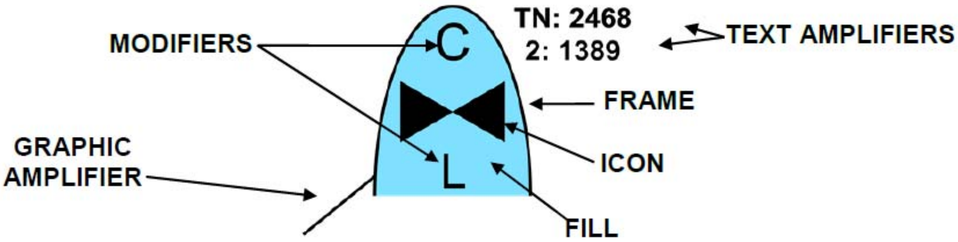

Figure 8: Air symbol composition [4]

6.6 SYMBOL IDENTIFICATION CODING SCHEME (SIDC)

A SIDC is a numeric string that can be used to provide the unique identifier to display or exchange symbol information between MIL-STD-2525 compliant systems. Figure 9 shows the 20 digit numeric SIDC. The first eight digits are used to identify the symbol set, i.e. version, standard identity, symbol set and status; while digit 9 and 10 are used for amplifier/descriptor, see Figure 10. The first ten digits are the minimum required number of digits to represent a symbol. Digits 11 – 20 describe the entity, entity type, entity subtype, first and second modifiers. Figure 10 shows the 10 additional optional SIDC for additional information.

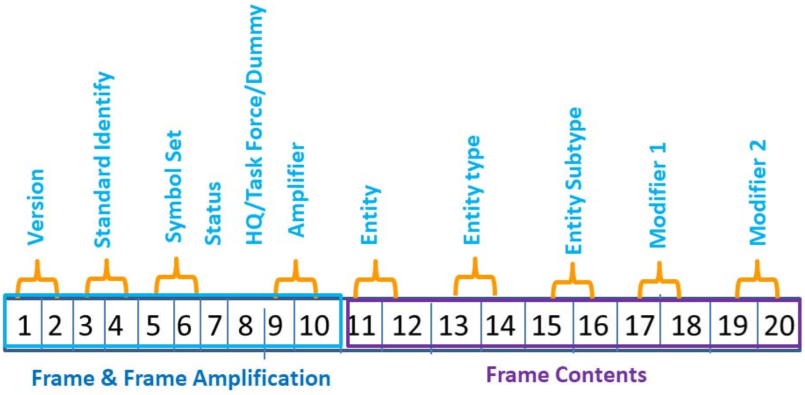

Figure 9: MIL-STD-2525D Symbology Identification Code (SIDC)

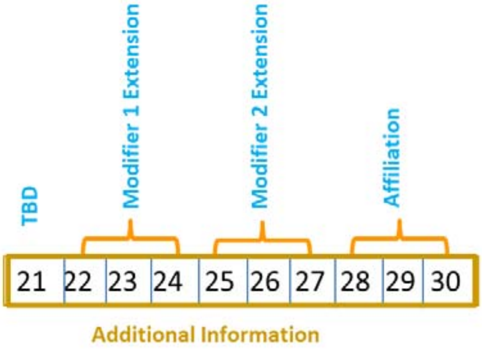

Figure 10: SIDC - Additional Information

The 20 digit SIDC code for the Air symbol composition in Figure 11 is 10030100001102000302. The C2/C4I system uses the SIDCs to construct the symbol from the library of the symbol parts to represent the object symbol.

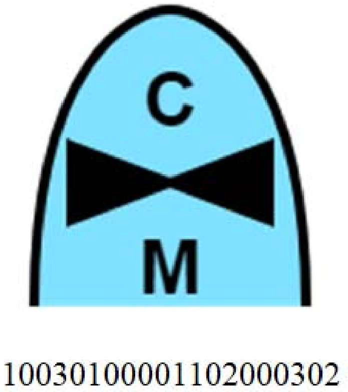

Figure 11: An air symbol example with its SIDC code

Figure 12 shows the application of the symbols on a geospatial map to depict the entities and thus understand the situation.

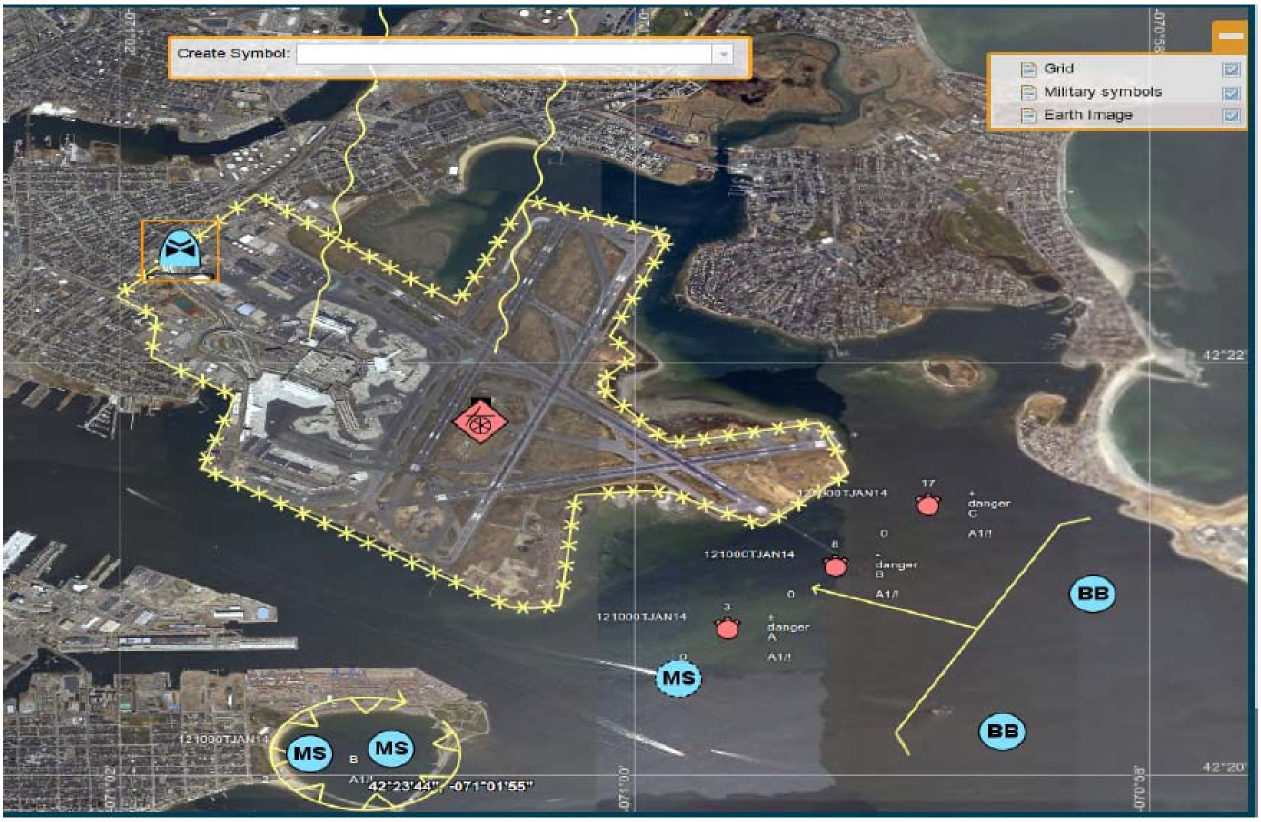

Figure 12: Visualization of Symbols [1]

6.7 Cyberspace symbols

An initial set of a small number of cyber symbols was published in the MIL-STD-2525D as Appendix L. The cyberspace symbols adopted the existing MIL-STD-2525 approach; they are constructed using the alphanumeric cyberspace icons. The idea is that by incorporating cyber symbols into MIL-STD-2525 and APP-6 then systems that already use these Standards will readily be able to use the new symbols.

Different cyberspace entity types have been enumerated: Botnet, Infection, Heath and Status, Device Type, Device Domain and Effect. Thus, for example, icon ‘BC2’ represents a Botnet in C2 and icon ‘AC2’ represents Advanced Persistent Threat (APT) in C2. The icon for Network Outage is ‘NOT’ for an ‘Effect’ entity, while the Network Outage icon for a ‘Health and Status’ entity is ‘OUT’. ‘XFL’ is the icon used to represent exfiltration for and ‘Effect’ entity.

The Joint Staff representation to the Symbology Standards Management Committee (SSMC) recognised there is a need to improve the initial set of cyber symbol published in Appendix L of MIL-STD-2525D.

The Joint Staff/J6 has set up the Cyber Symbology Working Group (CSWG) to conduct a study for the new cyber appendix. The CSWG identified that there are situational awareness gaps in the cyber operational aspects, and recommended the need of a common cyber symbology set for situational awareness within the COP. They chose MIL-STD-2525 as its basis since it is an established standard for military symbols. The CSWG has developed a Cyberspace Modifier, CYB, to enable the integration and synchronization of cyber operations with other domains. This will be used to represent the cyberspace element for existing and future Land, Sea, Air and Space symbols [13].

6.8 CYBER SYMBOLOGY MANAGEMENT

The user community is responsible for the development and testing of individual cyber symbols, while the Symbology Standards Management Committee (SSMC) and the NATO Joint Symbology Panel (JSP) are responsible for the majority of the cyber symbology management, such as review and approval of symbology proposals, control of the digital SIDCs and the symbology portrayal rules, symbology library management as well as the Standards documentation management. McGrane *et al.* recommended the inclusion of Human factors during the development and testing phases of cyber symbology to mitigate the problem in ambiguous symbols which are open to interpretation and / or data overload. Furthermore, they recommend that systems must be able to use SVG (Scalable Vector Graphics) format implemented in XML (Extensible Markup Language) [2 and 13].

7.0 OPERATIONAL GRAPHICS FOR CYBERSPACE

McCroskey & Mock identified the problems arise from the lack of effective communication between the physical and cyber domains which mean that decisions on strategic and mission planning will be made without being aware of the network situation that could endanger warfighters [12]. They developed a MIL-STD-2525 compliant symbol set that that addresses the display of cyber information in the Logical and Persona layers of cyberspace [9 and 12]. In McCroskey & Mock individual networks are represented by the devices they comprise, enclosed within a boundary of the IP address space. In order to reduce clutter only a small number of the devices are typically displayed as a representative.. Each network is uniquely identified by a different color. The distance between two networks is typically measured in terms of hops, c.f. physical distance. Time to travel between two nodes does not really represent distance accurately because it can be affected by short-term congestion and other network issues. Furthermore, cyber terrain is dynamic and on short timescales. Figure 13 shows a cyberspace terrain, squares represent individual workstation or client, circles represent servers, whereas a firewall is represented as a fortification, and a string of sensors are used to represent intrusion detection equipment. Red shading is used to indicate that the device is under the enemy's control or invaded.

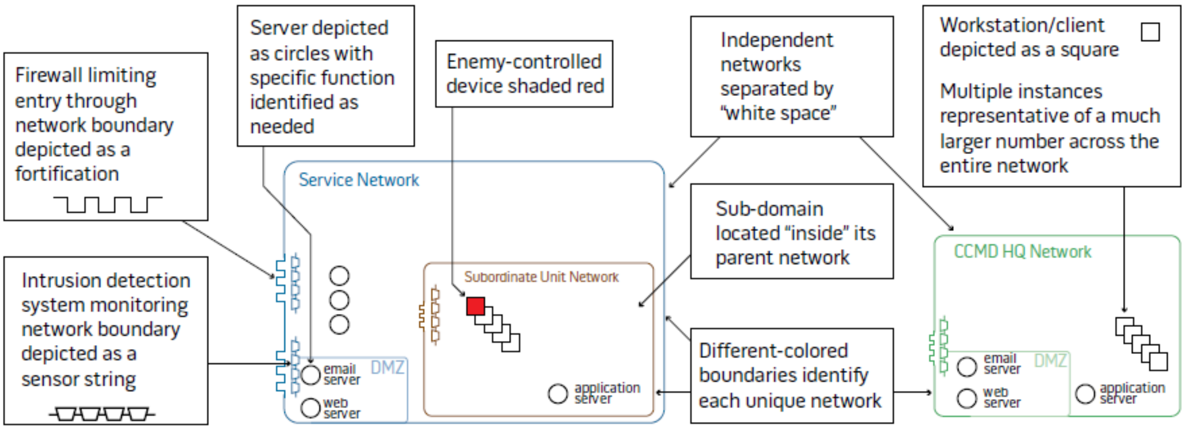
Firewall limiting entry through network boundary depicted as a fortification
Intrusion detection system monitoring network boundary depicted as a sensor string
Server depicted as circles with specific function identified as needed
Enemy-controlled device shaded red
Independent networks separated by "white space"
Workstation/client depicted as a square
Multiple instances representative of a much larger number across the entire network
Sub-domain located "inside" its parent network
Different-colored boundaries identify each unique network
Service Network
Subordinate Unit Network
CCMD HQ Network
DMZ
email server
web server
application server
DMZ
email server
web server
application server
application server

Figure 13: Cyberspace Terrain Description: Networks and Common Features [13]

McCrosky and Mock considered the Persona Layer to be composed of accounts and their associated credential such as usernames, passwords that enable users to gain access and conduct activities in the network. Accounts are therefore devices used by the human in the Physical Domain through the Logical and Persona Layers. The cyber units reside in two domains, firstly the users and the physical layer hardware domains, and, secondly, a combination of accounts, credentials, cyber actions and missions in another domain. Indeed they considered that the credentials are the keys needed to gain access to the cyber equipment and associated accesses and privileges. Keys are therefore used to represent different levels of credential, yellow key represents user, purple key for system-level and green key for domain-level. Hexagons are used to represent operations that occur only in cyberspace; such a representation is not, at present, available in MIL-STD-2525D. The hexagon is coloured using the standard colour scheme for friendly, neutral, hostile, civilian and unknown, but it is rotated by 30° for hostile units. Cyber units are based on three mission categories: a lightning bolt represents Offensive Cyberspace Operations (OCO), a shield icon for Defensive Cyberspace Operation (DCO) and existing support unit iconography for DODIN (Department of Defense Information Network) operation units. Figure 14 shows a sequential action in the in initial adversary assault with a feint, blocked phishing attack, a successful bypass of defences that lead to gaining control of the friendly terrain [13].

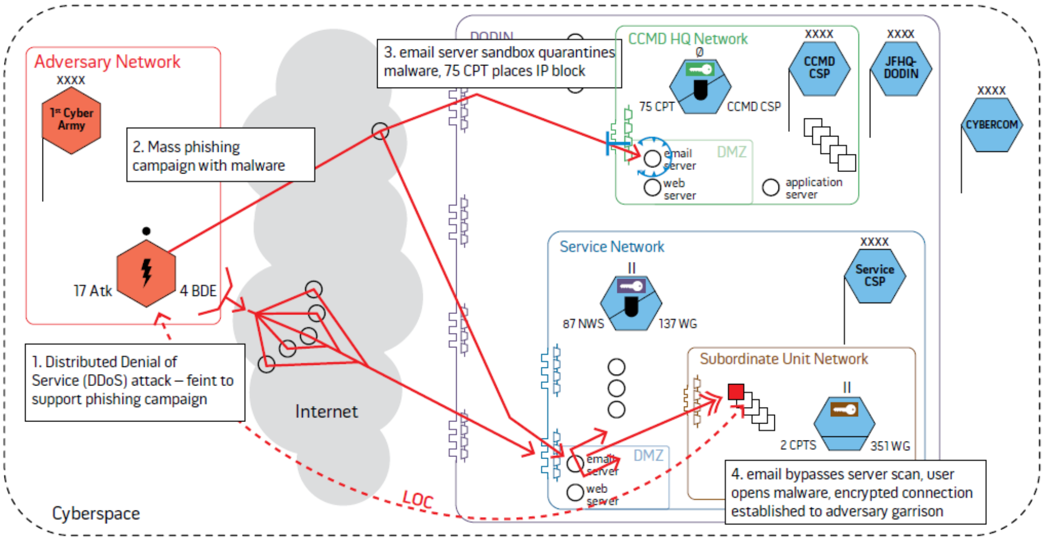
Adversary Network
XXXX
1st Cyber Army
2. Mass phishing campaign with malware
17 Atk
4 BDE
1. Distributed Denial of Service (DDoS) attack – feint to support phishing campaign
Internet
LOC
Cyberspace
DODIN
3. email server sandbox quarantines malware, 75 CPT places IP block
CCMD HQ Network
Ø
75 CPT
CCMD CSP
XXXX
CCMD CSP
XXXX
JFHQ-DODIN
XXXX
CYBERCOM
email server
DMZ
web server
application server
Service Network
II
87 NWS
137 WG
XXXX
Service CSP
Subordinate Unit Network
II
2 CPTS
351 WG
email server
DMZ
web server
4. email bypasses server scan, user opens malware, encrypted connection established to adversary garrison

Figure 14: Sequential Action in the initial Adversary Assault [13]

The objective of the cyberspace operational graphics is to provide a means to convey cyber information that is relevant to commanders who are unfamiliar with the technical aspects of the cyberspace that affects his decision making.

8.0 NETWORK PERFORMANCE

In any part of the Commander's C2 network, there might exist thousands or more computers and associated network components. The complexity of such networks makes them extremely difficult for humans to understand, protect and defend. Adversaries are perpetually trying to exploit networks for their own gain which could be stealing IPs, information or simply disrupting the network. Among the challenges are how best to analyse and visualize the massive volume of network data to detect potential malicious anomalous network activities. It is important to differentiate anomalies in the network that are due to network's misconfiguration or updates from those anomalies with malicious intent.

Figure 15 shows a display for monitoring the network system performance [18]. The calculation of the dynamics per log-file entry allows the application of spider diagrams to show the deviation of frequencies from average for log-entries containing the IP of an own host during specific time intervals. With every log-entry not only are the summarized dynamics saved, but also the dynamics for every specific value contained in the log-entry. In this way it is possible to calculate, for every host, for a selected time interval, the means of every parameter across all log-entries referencing this host. Spider diagrams are used as a symbol to visualize the dynamics of all the parameters on a map of the internal network for each internal host. This provides an intuitive means for the user to see problem readily as they arise, and thus make informed decision to mitigate the problems.

The application of spider diagrams in this context is very similar to the manner they have been used in other domains such as the monitoring of power plants. The spider diagrams not only show the deviation of parameters of each host, but they also show characteristic shapes for different states, and these may be recognized easily by an experienced operator. Such visualization facilitates first steps in providing diagnostics information. A heat map colour scheme can be employed to indicate how often the host occurs in the filtered log-entries, e.g. red for high frequency and blue for low frequency etc.

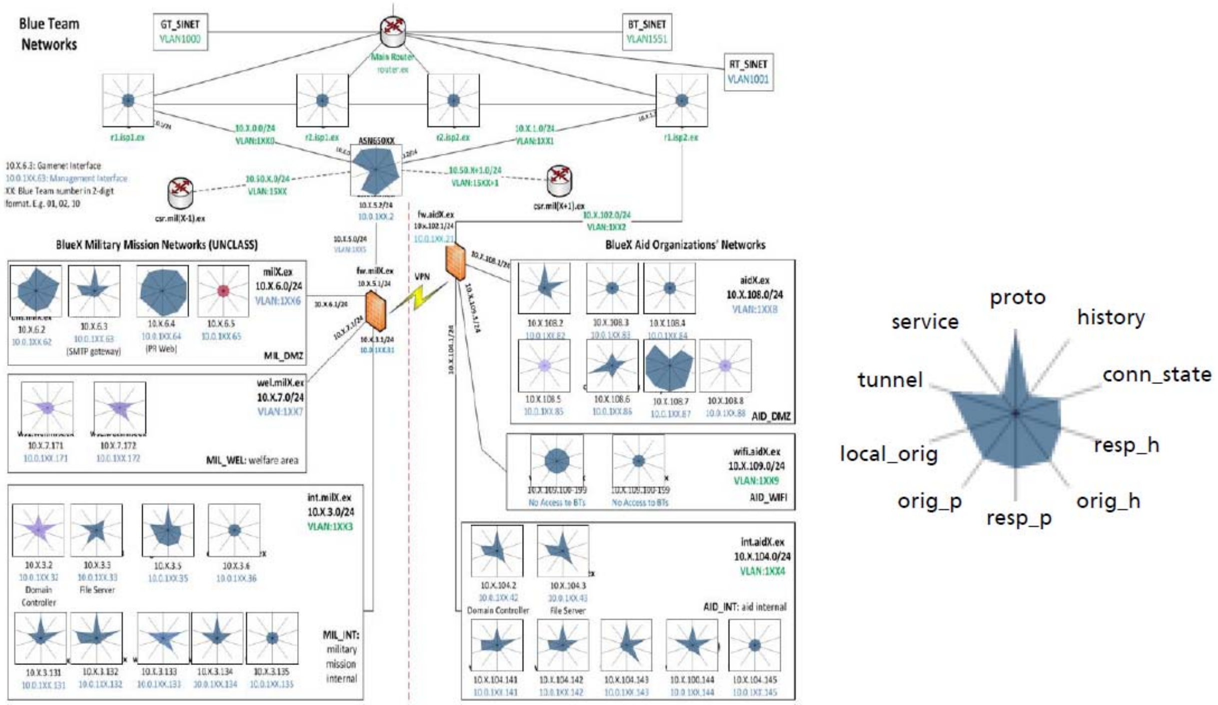

Figure 15: Spider Diagram - diagrams to show the footprint of the derivative behaviour for hosts in the own network [19]

This provides an effective means of communicating the status of the logical network.

9.0 JCD STORYBOOK SYMBOLOGY

Fugate & Gutzwiller identified the problem in treating cyberspace representation as a subset of the physical domain operational picture is that the characteristics of the physical domains differ from the cyberspace operations: for example, cyber effects and scanning operations are not physically visible and may not be physically co-located. Furthermore, re-using the physical space for cyberspace (MIL-STD-2525D) makes it difficult for users familiar with the physical domain and representation to differentiate the two; this results in treating cyberspace information as physically based information, i.e. mis-interpreting the information leading to mis-informed decision making. They raised their concerns in the following areas:

1. Geography and locality focused symbology, i.e. where but not why or how
2. Key visual discriminators – need to focus on control, c.f. ownership
3. Cyber entity density – complexity
4. Adjacency and defining cyber area of responsibility – Logical and physical network

representations
5. Effects and methods of action – not indicated in MIL-STD-2525D
6. Tiered symbology and displays – different symbology for users with different objective and needs
7. Fluidity of entity type – address multi-purpose entity

They explored alternatives for cyber symbology applied to cyber incidents, all with the premise of not being restricted to the design approach of the existing 'pre-cyber symbology' with its inherent assumptions, i.e. while being inspired by MIL-STD-2525 they did not restrict their approach to using physical domain symbology to depict cyber effect and actions for cyber threats [7]. Instead they considered that a cyber attack incident reflects the attacker's approach and motivation and use three symbols to represent three different entities in a cyber incident, namely devices, users and software, see Figure 16. They represent a device by a square, while a circle represents a user and a hexagon represents software. Vulnerability in a device is indicated by a broken outline. Each entity is also associated with a trust element, which can be unknown, trusted, untrusted, threat or insider.

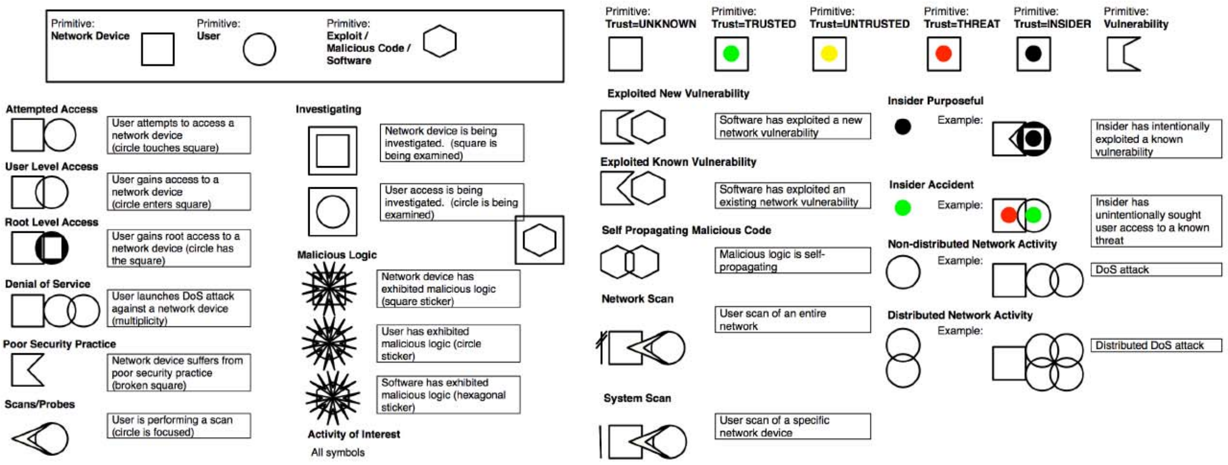
Primitive:
Network Device
Primitive:
User
Primitive:
Exploit / Malicious Code / Software
Attempted Access
User attempts to access a network device (circle touches square)
User Level Access
User gains access to a network device (circle enters square)
Root Level Access
User gains root access to a network device (circle has the square)
Denial of Service
User launches DoS attack against a network device (multiplicity)
Poor Security Practice
Network device suffers from poor security practice (broken square)
Scans/Probes
User is performing a scan (circle is focused)
Investigating
Network device is being investigated. (square is being examined)
User access is being investigated. (circle is being examined)
Malicious Logic
Network device has exhibited malicious logic (square sticker)
User has exhibited malicious logic (circle sticker)
Software has exhibited malicious logic (hexagonal sticker)
Activity of Interest
All symbols
Primitive:
Trust=UNKNOWN
Primitive:
Trust=TRUSTED
Primitive:
Trust=UNTRUSTED
Primitive:
Trust=THREAT
Primitive:
Trust=INSIDER
Primitive:
Vulnerability
Exploited New Vulnerability
Software has exploited a new network vulnerability
Exploited Known Vulnerability
Software has exploited an existing network vulnerability
Self Propagating Malicious Code
Malicious logic is self-propagating
Network Scan
User scan of an entire network
System Scan
User scan of a specific network device
Insider Purposeful
Example:
Insider has intentionally exploited a known vulnerability
Insider Accident
Example:
Insider has unintentionally sought user access to a known threat
Non-distributed Network Activity
Example:
DoS attack
Distributed Network Activity
Example:
Distributed DoS attack

Figure 16: The JCD Storybook Symbology which uses individual boxes to indicate entity, colours for trust, and visual analogy for the way these systems interact to form a cyber incident [7]

Figure 17 shows an example of a cyber incident using the JCD Storybook Symbology.

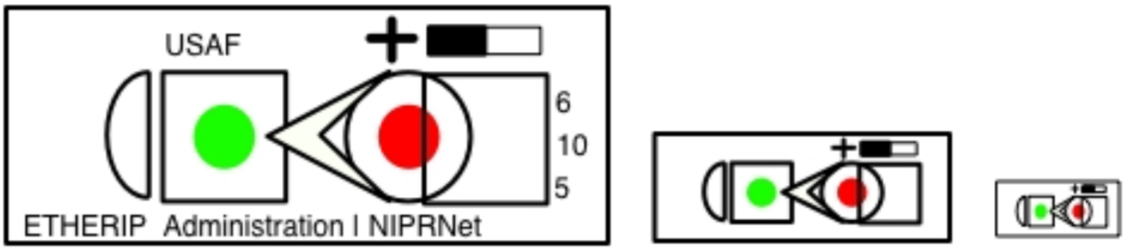

Figure 17: An example of how the JCD Storybook Symbology might describe an incident — A trusted USAF NIPRNet webserver used for administration was TCP scanned by an untrusted user from a machine with unknown trust. The hypothetical incident is classified secret and of moderate severity [7]

They concluded that there is the need to determine what to display, how to display it and conduct an evaluation to see if it improves decisions and understanding in the cyber domain.

10.0 DISCUSSION

This paper has briefly explored the research, development and exploitation of symbols in depiction of cyber situation. Among the challenges are how to represent the COP consisting of the Physical, Logical and Persona layers in a collective separable manner, i.e. being able to separate each of their status and impact in their combined situation so as to understand how a problem relates in the different layers. Furthermore, the users from the three tiers have different tasks and needs, but they are facing the same situation; so, there is a need to consider how to transition and translate seamlessly the symbology between different tiers so that information is shared throughout the tiers. The following are the challenges:

- How to decide what is the intuitive way to depict multiple cyber elements and their associated situations?
- How to decide what is the intuitive way to depict multiple cyber situations?
- How much information and detail are necessary for and from different user groups and different operational needs?
- How to show the temporal elements of a situation?
- How do icons compared with symbols in conveying the required information?
- When to use icons and in what operations / activities / domain(s)?
- When to use symbols and in what operations / activities / domain(s)?
- Should we still superimpose the symbol on a geospatial map and / or should other aspects such as the network architecture be included?
- How can user performance be evaluated?

10.0 References

[1] Andrews, M. and Loveridge, S., Joint Symbology Standard Management in the military domain, NATO IST-HFM-154 Specialists' Meeting on Cyber Symbology, 28th – 30th November, 2016.

[2] Conti, G., Nelson, J., Raymond, D., Towards a Cyber Common Operating Picture, 5th International Conference on Cyber Conflict, K. Podins, J. Stinissen, M. Maybaum (Eds.), NATO CCD COE Publications, Tallinn, 2013.

[3] https://www.army.mil/article/152979 (DARPA' Plan X)

[4] Department of defense interface standard joint military symbology, MIL-STD-2525D, 10 June 2014.

[5] Endsley, M. R., Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1): 32-64, March, 1995.

[6] Endsley, M. R. and Jones, D. G., Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition, CRC Press, 2004, ISBN 9781420063554.

[7] Fugate, S. F., and Gutzwiller, R. S., Rethinking cyberspace symbology, NATO IST-HFM-154, Cyber Symbology Specialists' Meeting, USA, November 2016.

[8] Jawhara, I., Mohamedb, N., Jameela Al-Jaroodic, J., Agrawald, D. P. and Zhang, S. Communication and networking of UAV-based systems: Classification and associated architectures, Journal of Network and Computer Applications 84, pp 93–108, 2017.

[9] Joint publication 3-12, Cyberspace Operations, 8 June 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (retreived 26 May 2019)

[10] Kilgore, R., Godwin, A., Hogan, C., Davis, A., Pfautz, J., Woods, D. D., Branlat, M., and Kaufman, H., Tangible Trustworthiness for Mixed-Initiative Network Defense. SBIR Phase I Final Report, 2012.

[11] Lanham, M., Cyber Defence Planning: Operating on Unconventional Terrain, Army Communicator, pp 7-12, 2012.

[12] McCroskey, E. D. and Mock, C. A., Operational Graphics for Cyberspace, Joint Force Quarterly 85

[13] McGrane, B., Bohling, J. and Epler, M., Development, Distribution and Management of a Common Cyber Symbology for Joint Military Planning and Operations, NATO IST-HFM-154, Cyber Symbology Specailists' Meeting, 28th – 30th November 2016, Ohio, USA.

[14] NATO APP-6, http://nso.nato.int/nso/zPublic/ap/PROM/APP-6%20EDD%20V1%20E.pdf, (retrieved 27 May 2019).

[15] Rogers, Y, Sharp, H. and Preece, J., Interaction Design: Beyond Human-Computer Interacton (2nd edition). New York, NY: John Wiley & Sons, Inc. 2007.

[16] Varga, M. J., Winkelholz, C., Träber-Burdin, S., Liggett, K., Werner, K. , Bivall, P. and Lavigne, V., A Consideration of the Application of Icons and Symbols in Cyber Situation Awareness, NATO IST-HFM-154 Cyber Symbology Specialists' Meeting, 28th – 30th November 2016, Dayton, USA.

[17] Wickens, C. D., Lee, J. D., Liu, Y. and Gordon-Becker, S., Introduction to human factors engineering, 1998.

[18] Winkelholz, C., Chapter 6: Cyber Defence - Visualizing and Analyzing Netflow Logfiles, Visualization for Analysis (NATO STO-TR-IST-110), pp 67 – 75, 2018.