PHOTO: SSG SHAWNON LOTT

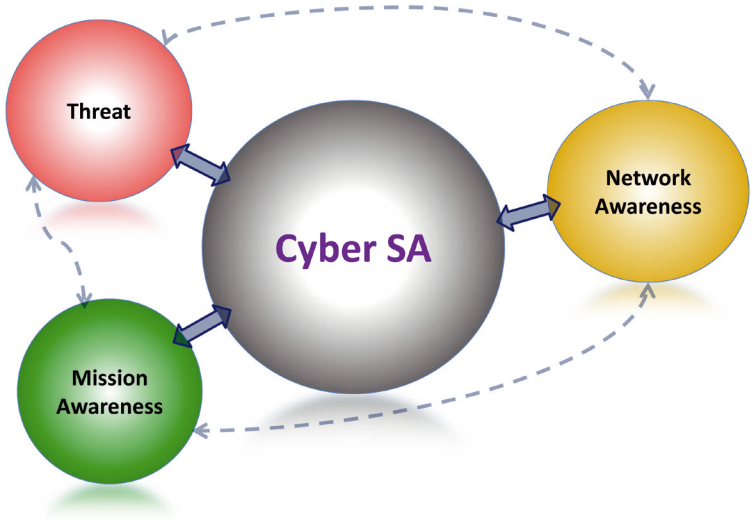
CYBER SITUATIONAL AWARENESS FOR THE NATO ALLIANCE

by **COLONEL RIZWAN ALI**
United States Air Force
Team Leader, Task Force Cyber
Supreme Headquarters Allied Powers Europe (SHAPE)

CYBER SITUATIONAL AWARENESS is often times referred as the "holy grail" of cyberspace. This is because there isn't any consistent definition, methodology or even an industry recognized framework of what constitutes cyber situational awareness. Academic that we have consulted, have referred to this as a "wicked problem", something that is difficult or impossible to solve because of incomplete, contradictory or changing requirements that are often difficult to recognize. For the past two years, we at NATO's Supreme Headquarters Allied Powers Europe (SHAPE) have taken on this challenge of solving this "wicked problem". Through this effort, we have been setting the standard of how to conceptually think of cyber situational awareness.

On the surface, the problem seems quite simple to solve, but just below the surface, the complexities are revealed. Many organizations have some type of mechanism to gather relevant metrics and threat data, which either their network technicians or some level of middle management use to make their decisions. However, most of these organizations have developed these lists of metrics through an ad hoc method, rather than starting from a conceptual framework of how to visualize what their key decision-makers need in order for them to make strategic decisions. Also, many have not consulted with the senior decision-makers to ensure the metrics they are gathering meet these leaders' information requirements.

Figure 1: Cyber Situational Awareness Framework



The Challenge of Aggregating the Data

If we take a look at the typical large organization, such as a commercial entity, a governmental agency, or even an international organization such as NATO, we see it is very likely there are a significant number of reports being generated to support cyber situational awareness. These reports range from high-quality to low-quality; from high-reliability to low-reliability; and from technical-level to strategic-level. These reports are produced by dedicated people who firmly believe their analyses are definitive, authoritative and represent the cyber situational awareness view, which strategic leaders need to aid their decision-making process. Very often these pockets of cyber situational awareness entities do not know that other reports supporting cyber situational awareness are being generated elsewhere in their own organizations.

Even in the cases where some knowledgeable employees know that other reports exist, the task to aggregate and analyse the reports is far too complex to undertake without dedicated personnel and strategic direction on "how" to aggregate and analyse these myriad of reports. The unfortunate fact is the data aggregation challenge often revolves around not having a sound framework on what is required by the senior leadership of an organization to base their decisions upon. All too often, the development of this strategic framework is left to technicians and engineers who may not be aware of the strategic needs of the senior leaders. The challenge of developing a cyber situational awareness framework is a leadership issue, not something that can or should be delegated to technicians to solve.

Lack of an Industry-Standard Cyber Situational Awareness Framework

At SHAPE, we faced the exact scenario described above. There seemed to be a dearth of information, lack of data aggregation, and the absence of a cyber situational awareness framework endorsed at the General Officer level. We discussed this issue with a number of senior decision-makers internally in SHAPE and at NATO HQ. We also had extensive discussions with industry up to the Chief Technology Officer, Chief Information Officer and Chief Executive Officer levels. We contacted senior governmental officials and even consulted with prominent academics who have thought deeply about this "wicked problem". Each of these interactions was useful, but they didn't yield the elusive cyber situational awareness framework that we could use within NATO and SHAPE in order to provide our key decision maker with relevant, decision-quality information.

Varied Views of What Constitutes Cyber Situational Awareness

If we were to take a survey of attendees at a typical cyber security conference, and ask them what they think is meant by cyber situational awareness, we would get dozens of answers. Most of them would likely be valid. This is because cyber situational awareness means different things to different people.

For our network operators, cyber situational awareness means ensuring firewalls and other hardware and software are properly configured and system patches are all current. They would also note that they would need to effectively monitor the systems and networks for anomalies and then develop a series of metrics to help them determine trends over time. The network operators would likely make use of automated tools and interface with industry to determine what changes or unusual activities are happening in the global internet, which may have an impact on the organization's networks. For many organizations, this is sufficient. However, for an international military alliance like NATO, this is only a part of the cyberspace picture.

For our intelligence analysts, cyber situational awareness means identifying the threat actors. They utilize a variety of methods to determine who the threat actors are for an organization. These can be nation-state actors, criminal groups, hacktivists, or even malicious insiders. These analysts would traditionally gather information from multiple sources to include open sources like press reports, classified and unclassified reports from governments, analysis from companies that specialize in cyber situational awareness and malware campaign analysis produced by specialized en-

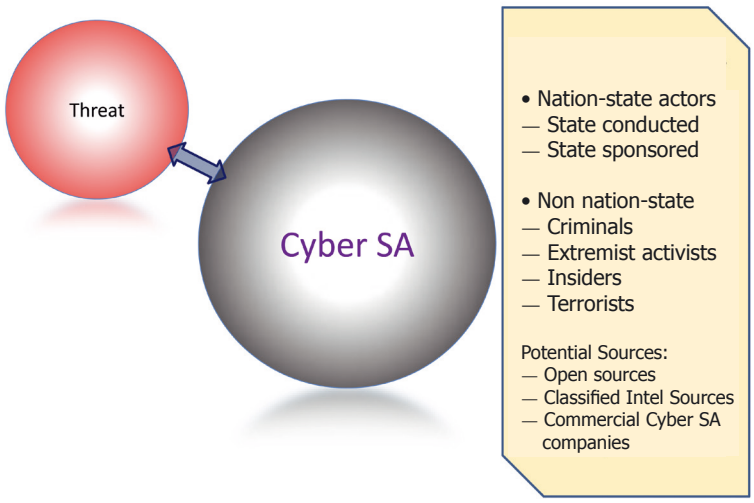
gineers. Again, for NATO, this portion of the cyber picture in important, but it is not complete. Finally, from a military perspective, NATO's operational commanders need to know how well defended are their mission networks. This would involve performing a full vulnerability assessment, determining single points of failure, and the training level of their cyber staff as well as the cyber threat awareness level their entire staff. But, beyond the technical and training aspects, the operational commanders would also need to know how well their staff is able to operate in a degraded and denied cyber environment. Frankly, cyber situational awareness is a bit of a jigsaw puzzle. Each of these various aspects of cyber situational awareness is correct, though not complete. After all these discussions, and considerable analysis, we believe we have come up with a cyber situational awareness model, which will meet the needs of SHAPE and possibly many other national defence organizations.

SHAPE's Cyber Situational Awareness Framework

For SHAPE, we believe that cyber situational awareness has three major components (Figure 1). Each of these components is important in helping us build a fuller cyber situational awareness picture for our senior leaders. They are:

- Threats
- Network Awareness
- Mission Awareness

Figure 2: The Threat Component



We categorize strategic-level threats (Figure 2) into two categories: nation-state actors and non-nation-state actors. Nation-state actors can conduct cyber operations themselves or through actors that are state-sponsored. Non-nation-state actors include criminals, extremist activists, insiders and terrorists.

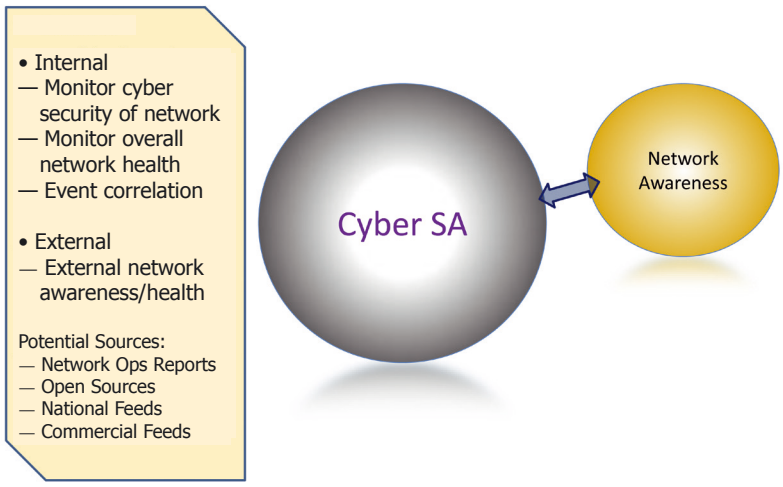
Some of you may notice the technical threats such as viruses, malware, ransomware, etc., are missing from the list. That's because these are vectors that nation-state and non-nation-state actors may use in cyberspace, not threat-actors in and of themselves. In many cases it is difficult to differentiate between nation-state and non-nation-state actors due to the increased technical sophistication of non-nation-state actors. Potential sources for this type of situational awareness include:

— Open Sources, such as press reports and academic analysis,
— Classified intelligence produced within NATO and supplied by the Alliance members,
— Cyber situational awareness reports produced by commercial companies.

The network awareness portion of SHAPE's view of cyber situational awareness is technically focused (Figure 3). Typically, when computer information systems (CIS) personnel talk about cyber situational awareness, this is what they focus on. But for SHAPE, network awareness is just one component of cyber situational awareness. For the internal NATO networks, we believe cyber situational awareness entails monitoring the cyber security of the network, monitoring overall network health as well as doing correlation of various incidents on the network to determine if there is a trend or persistent threat acting on our networks.

Since NATO is an international organization, for us being aware of major changes or incidents to the global internet is also important. An example of this would be the discontinued support for the Windows XP operating system. Though our network defenders fully addressed this issue for our internal NATO networks, it was important for us to know how this impacted the overall global internet and what implications there would be to NATO

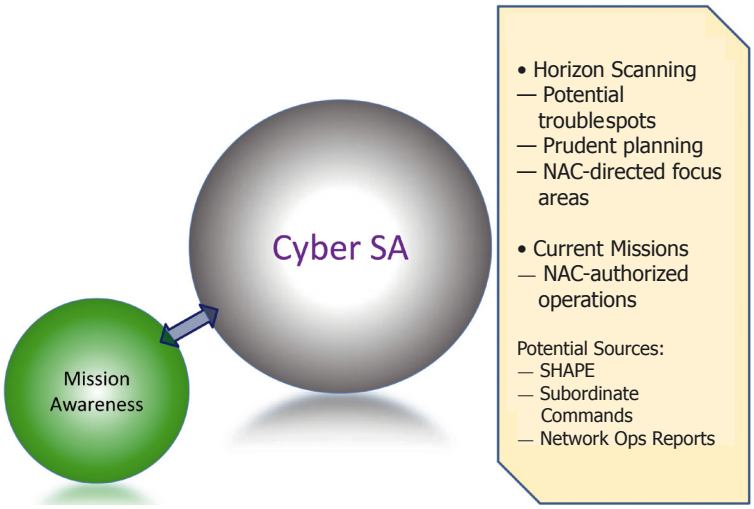
Figure 3: Network Component



networks from unsecured Windows XP systems outside NATO.

Then finally, for SHAPE, we need to monitor our ongoing mission areas (Figure 4). This is an important facet of our cyber situational awareness that often gets overlooked if viewed only from a technician or intelligence perspectives. We need to provide the necessary horizon-scanning, from a military perspective, to the North Atlantic Council (NAC). We also need to be aware of any cyber issues related to current NAC-authorized operations that Allied Command Operations is conducting.

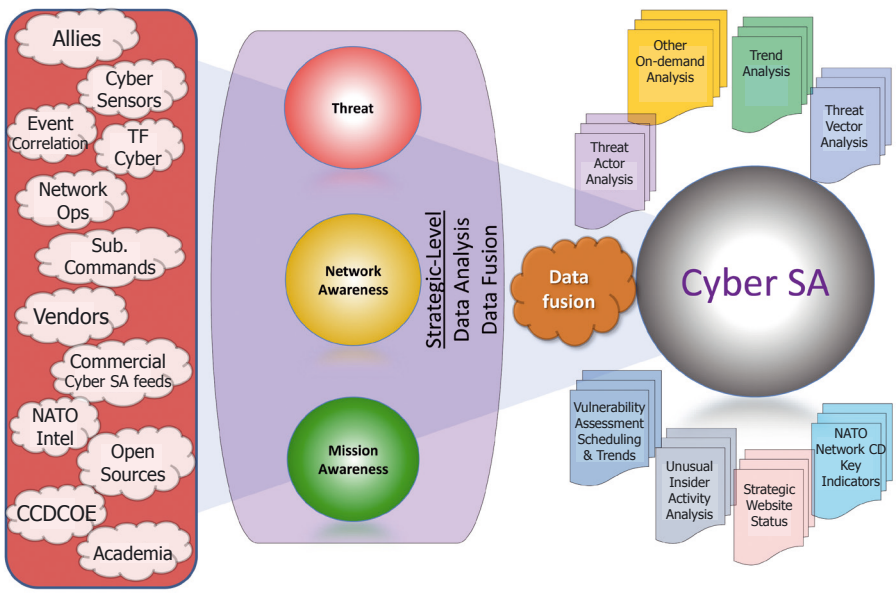
Figure 4: Mission Awareness Component



Putting It All Together

What I have described above is still not complete. The final piece required is to aggregate the various cyber situational awareness information presented by the threat, the network, and the mission components of the framework. This should be done by a dedicated team who can present this information in ways that can be easily understood by key decision makers. Only when this final piece, the data aggregation, is completed can this be presented as a true cyber situational awareness framework (Figure 5). When you put together all these different pieces of what constitutes cyber situational awareness, you end up with a fused picture, which can be applied to the common operating picture the key decision makers need. For SHAPE, the entity that we use to do the data aggregation is Task Force Cyber. Task Force Cyber is made up of a mix of personnel who are trained to operate at the strategic level, but still have the necessary technical and military skills to make sense of the data generate reports, which provides the Supreme Commander Europe (SACEUR) with the strategic context to the cyber data that he is presented. The process of providing SACEUR with the strategic context to the cyber data is not easy. The training and dedication of the officers and civilians involved with this key part of the cyber situational awareness framework has be to impeccable.

Figure 5: Putting It All Together



Conclusion

Through this careful analysis we believe we have solved the "wicked problem" of the cyber situational awareness framework. Making the effort to effectively define the problem and then developing a conceptual framework was critical for SHAPE. Though this framework (Figure 1) looks simple, it took a significant amount of time to conceptualize, and it represents a major milestone for NATO.

At SHAPE, we believe that this is the first cyber situational awareness framework that has ever been developed that is relevant to a defence organization. The framework has been well received when briefed to NATO Member Nations at various forums. It was also validated as an appropriate and relevant framework by an independent analysis conducted by a major industry partner at our request.

We are using this framework daily to help organize the activities of cyber team members within SHAPE and in our subordinate commands. SHAPE's framework is simple and malleable enough that it can be easily adapted and used by Alliance Members as a basis for their own national framework. It can also be easily adapted to other organizations that need a cyber situational awareness framework. ✦