Sharing Cyber Capabilities within the Alliance

X

Interoperability Through Structured Pre-Authorization Cyber

By Dr Jan Kallberg, Research Scientist, Lieutenant Colonel Todd Arnold, Research Team Lead, and Colonel Stephen Hamilton, Technical Director
United States Army Cyber Institute at West Point

Introduction

Sharing cyber weapon/cyber capabilities requires trust between the member states, becoming a high-end policy decision due to the concerns of proliferation and the investment in designing a cyber-weapon that has a limited 'shelf-life'. The digital nature of cyber weapons creates a challenge. A cyber weapon can spread quickly, either self-propagating such as worms or via disclosure (and subsequent reuse) by malware researchers or malicious actors, raising proliferation concerns. Additionally, a cyber-weapon can be copied by the adversary or reverse engineered. Once the weapon is released, the adversary will eventually address the vulnerability, and the opportunity is gone. These factors raise the threshold between member states to share cyber weapons and cyber capabilities. Alliances, like NATO, prepare for a unified multinational, multi-

domain fight; meanwhile, the national cyber forces are still operating as solitaires with limited interoperability and sharing. There is a need in the collective defence posture to integrate the multinational cyber force to achieve interoperability.

Time

The NATO framework such as the Sovereign Cyber Effects Provided Voluntarily by Allies SCEPVA[1] lays a foundation, but there are two obstacles – time and the concept of voluntarily enabling others. First, there is an expectation that future conflicts will unfold rapidly, as evidenced by the Russian invasion of Ukraine on 24 February 2022. It is doubtful that there will be the time[2] in conflict to communicate between member states seeking a voluntary release of cyber capabilities. Secondly, the voluntary provision for support to the mission requires that the provider be willing to provide the cyber capability, and there is a sharing of needs followed by a decision process. These hurdles will take days, or even weeks, to sort out. The narrowing time window to share cyber capabilities requires a framework for sharing between member states based on existing trust and relationships. There is also a risk that the adversary will repurpose and reuse the cyber weapon, leading to unintended consequences and lateral movements.

Solving Trust, Obligation, and Narrow Time Window

The concept of collective defence assumes an obligation to provide a cyber-capability. The Alliance multinational force seeks interoperability, but the national cyber forces are still tied to the member state's mission instead of the joint collective defence. The tenets of cyber capabilities hinder their rapid sharing because the weapons represent a significant time

and resource investment for the provider. Effective tools require finding a vulnerability, weaponizing the opportunity, and once launched, the targeted adversary can nullify the weapon through patching and countermeasures. The provider has an understandable doubt about sharing these cyber weapons, especially under time pressure and without fully understanding how the cyber weapon will be handled by the receiving member state's cyber force.

In European and transatlantic politics, friendly nations mitigate distrust by arrangements that accept a variety of trust levels. Both the European Union and NATO have a history of cross-border dialogue, seeking common ground, and engaging in discussions of formalized relationships between friendly nations. There is a negotiation and hopefully an agreement. Even in computer security, there are negotiations between nation-states of mutual acceptance and agreements. The (ISO/IEC 15408) Common Criteria[3] framework is described by German certificate issuer TÛV Rheinland[4] as; 'It is a framework that provides criteria for independent, scalable and globally recognized security inspections for IT products.' In the Common Criteria framework, friendly nations negotiate the level of acceptance of another country's information security evaluations and enter binational agreements.

We propose that friendly nations, within a structured framework, negotiate cyber capability sharing pre-conflict. Our 'Framework for Pre-Authorized Joint Cyber Mobilization' is inspired by the success of the (ISO/IEC 15408) Common Criteria. Mutually accepted hardware security certifications as the Common Criteria face the same challenge as sharing cyber weapons of navigating trust, operational reality, and risk. The proposed framework for pre-authorized multinational cyber weapon sharing in a mixed trust environment utilizes the experience and structural concepts of the (ISO/IEC 15408) Common Criteria framework. The framework's prearranged acceptance of foreign information security certified evalua-

tion. The Common Criteria, with defined levels of Evaluation Assurance Levels (EAL) ranging from 1 to 7, provides a framework that establishes trust levels between friendly nations. Critical to the proposed framework are transparency between partners, pre-conflict agreements and authorizations, specific limits to the extent of sharing cyber weapons, and responsibilities. Creating specific levels of cyber effects and the risks of collateral damages explains the cyber capability without comprising the actual utilization and functionality.

Our proposed cyber capabilities sharing framework will classify cyber capabilities by Expected Cyber Effect (ECE), Potential Lateral Uncontrolled Movement (PLUM), and Target Class (TC), which we will define in the subsequent sections.

Expected Cyber Effect and Potential Lateral Uncontrolled Movement

ECE and PLUM are vital components. ECE indicates what can be assumed to be achieved with the weapon. The classification for uncontrolled lateral movements assesses the chances for collateral damages, including potential hostile use of the tool once acquired/reverse engineered by the adversary. Each level's ECE level is described in Table A.

The second consideration – PLUM – is the ability of the cyber capability to act autonomously and potentially spread in an uncontrolled manner. The PLUM of a cyber-capability must be considered because, unlike collateral damage from kinetic weaponry, which has a limited physical range (not considering nuclear, biological, or chemical weapons which have a more extensive, but fundamentally limited effective range), cyber capabilities have the potential to spread rapidly and affect billions of devices connected to the Internet. Table B describes the PLUM for each level.

The ECE and PLUM levels are not 1:1; they must be considered independently. For example, a non-publicly known/released capability (Category 4 ECE) that affects low-priority targets can rapidly spread in an uncontrolled manner (PLUM 7). Despite the low ECE, the higher PLUM category will require guarantees in the negotiations that the receiving nation can safeguard and contain the cyber capability.

Category	Expected Cyber Effect
1	Known public tool, may be targeted with limited or medium effect
2	DoS, mass area of effect
3	Recently released or time sensitive usability (e.g. 1-day)
4	Non-publicly known/released capability (e.g., 0-day)
5	Targeted system capability, but requires (limited) physical access
6	Non-publicly known/released capability (e.g., 0-day) with high strategic importance
7	Highly targeted/specialized, non-publicly known/release capability (e.g., 0-day) with high strategic importance

Table A: *Allied Cyber Capability Sharing alignment of Expected Cyber Effect*

Category	Potential Lateral Uncontrolled Movement
1	Vulnerability is/should be patched, so will have limited spread and usability
2	Resources to make use of capability are required ahead of time, so limited uncontrolled movement
3	Requires wide distribution to make use of, due to imminent patching
4	Requires user interaction (e.g., phishing attack)
5	Requires little to no user interaction so minimal spread and highly targeted, but physical proximity limits usage
6	Requires little user interaction (e.g., watering-hole attack), so code must check for target system
7	Requires no user interaction (e.g., worm or remote), so spread must be checked in capability

Table B: *Allied Cyber Capability Sharing alignment of Potential Lateral Uncontrolled Movement*

Example Target Classes

The TCs – what can be affected by the capability – are defined within the framework to create uniformity in targeting definitions. As envisioned in the negotiations, the potentially receiving party puts forward a Targeting Request (TR), a well-defined request for a specific ECE against a specific TC. The providing party only presents TCs for a specific level of weapons. The presentation of the TC, and not capability, avoid spillage due to unnecessary information at the negotiating stage. For example, the receiving party puts forward a TR for the potential adversary's air defence system SAM-XXX and the providing party can reply with TC Air Defence. The provider knows in advance, what the receiver wants, and it becomes crucial to expedite the request in conflict and the execution of the agreement.

Examples of Member State's Pre-authorization Aligned with the Proposed Framework

Consider that pre-conflict, state X and Y agree to exchange cyber capabilities targeting Air Defence systems. State X agrees to share with state Y cyber capabilities up to ECE 5 and PLUM 3. State X's determining factors for acceptable levels are a concern regarding state Y's ability to safeguard the capabilities, primarily based on an assessment of cyber maturity, security controls, capabilities, and the impact on other systems if control of the capability is lost.

The acceptable levels between states may not be equivalent, and in this example, the risk appetite is different between states X and Y, which is reflected in the pre-authorization negotiation. Member state Y is only willing to share its high-level cyber capabilities by pre-authorizing up to ECE 3 targeting Air Defence to be shared with X. Member state Y considers itself to have a more secure cyber posture. Hence, a capability's potential lateral

Example preauthorization	Providing state	Receiving state	Expected Cyber Effect	Potential Lateral Uncontrolled Movement	Target Class
	X	Y	5	3	Air Defence
	Y	X	3	5	Air Defence

Table C: *Examples of sharing agreements between two member-states*

movement after use by X is of less concern to Y, so Y preauthorizes to X ECE 3 PLUM 5. These differences are reflected in Table C, which summarizes the pre-authorized sharing agreement between states X and Y.

While the states agree to pre-authorized levels, sharing or disclosing a capability's existence does not necessarily occur until one state requests a capability. In conflict, member state Y requests from member state X a cyber-capability targeting Air Defence at the highest level of the agreement: ECE 5 PLUM 3. State X delivers, without delay, a cyber-capability at ECE 5 PLUM 2, which is the highest-level capability targeting Air Defence available in X's arsenal and within the pre-coordinated levels.

Conclusion

The proposed framework is a model which naturally can be improved after further studies. The basis for the proposed framework is binational negotiations; NATO and EU states have experience and a history of numerous successful agreements. For example, NATO has established processes for defensive cyber operations whereby a member nation can request cooperation and assistance, but our concern is sharing mechanisms for offensive cyber operations. By agreeing to binational cyber capability sharing as a priority, response times can be reduced when a conflict arises, and a stronger response is possible within the Alliance. When rapid action

is required, it is of the utmost importance that events cannot unfold faster than the Alliance's decision cycle. We consider preauthorization as a functional way to mitigate that risk.

Dr Jan Kallberg is a Research Scientist at the Army Cyber Institute at West Point. He earned a PhD in Public Affairs (Government) and MA in Political Science at the University of Texas at Dallas and holds a JD/LLM from Stockholm University. Dr Kallberg holds ISC2 CISSP and ISACA CISM professional certifications.

Lieutenant Colonel Todd Arnold is a 2001 graduate of the United States Military Academy, West Point. His first assignment was to the 22d Signal Brigade in Darmstadt, Germany, where he twice deployed in support of Operation Iraqi Freedom. He is currently a Cyber officer, has held various technical positions, and was the first Lead Developer for the Army's Cyber Solutions Development Detachment at Ft. Meade, MD. He completed his PhD in Electrical Engineering from Columbia University in 2020 and joined the Army Cyber Institute, West Point, shortly after that to serve as a Research Team Lead and Assistant Professor in the Dept. of Electrical Engineering and Computer Science.

Colonel Stephen Hamilton is an Associate Professor at the United States Military Academy, a Cyber officer in the US Army and an extra class licensed ham operator, KJ5HY. He has deployed to Iraq as a signal company commander, and to Louisiana in support of Hurricane Katrina relief efforts. He has held various staff positions in signal and cyber units. Stephen is currently the Chief of Staff and Technical Director of the Army Cyber Institute. He holds a Bachelor of Science degree in Computer Science from the United States Military Academy, a Master of Science in Software Engineering from Auburn University, and a PhD in Computer Science from Johns Hopkins University.

Endnotes

1. Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations, Ministry of Defence (UK), p. 5. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (accessed on 10 January 2022).
2. J. Kallberg, and T. S. Cook, 'The unfitness of traditional military thinking in cyber,' IEEE Access 5 (2017): 8126–8130.
3. Common Criteria Portal, About the Common Criteria, [website], https://www.commoncriteriaportal.org/ccra/index.cfm (accessed on 10 January 2022).
4. TÜV Rheinland, Common Criteria Services – ISO 15408, [website], https://www.tuv.com/world/en/common-criteria-services---iso-15408.html (accessed on 10 January 2022).