Policy White Paper

Regional Program Political Dialogue South Mediterranean

Mediterranean Cyber Defense/Offensive Capacity Building- We are in it together:

Exploring cybersecurity collaboration between the two shores of the Mediterranean

Mr. Firas Sassi, Senior Director of National Security and Geo-Strategy Policy, IPASSS

Time is running out and countries ought to do more to create practical actionable solutions when it comes to cyberwarfare. Laws must catch up to the technologies being developed and deployed. Mutually beneficial capacity building initiative must be at the forefront of Mediterranean cooperation. We may be heading into a cyber-war and cyberspace is a jurisdiction of military.

States operating in the region are battling for superiority in the information space by using electronic warfare techniques. In 2017, total number of strategically important nation state driven cyber incidents targeting meditteranean countries was 18. In 2018 and 2019, the number of incidents sharpely increased to 32 and 38 respectively.[1]

Konrad Adenauer (KAS) and the Institute for Prospective and Advanced Strategic and Security Studies (IPASSS) are working to influence government to share knowledge, build capacity and structure a draft for an achievable Regional Cyber Warfare Treaty.

Cybersecurity is a rapidly growing concern to states and governments, globally and in the Southern Mediterranean region. Outdated security precautions are being targeted by cybercriminals and nation state actors; discussing ways to Improve and strengthen cybersecurity posture and resiliency is rightly a top priority for the MENA region and Europe.

Reviewing the current dimension, cyber space is turning into a theater battlefield for geopolitical interaction. Multiple cases as seen in Libya, Syria, and Yemen, which had turned into digital battlegrounds as foreign actors, intervened to exacerbate the ongoing conflicts, with cyberattacks, propaganda and disinformation.

Impediments to invest in and foster cyber security outlined in our latest webinar[2] as decisions to invest in cybersecurity require cost allocation and resource that are not always available. In addition, enhanced level of cybersecurity can conflict with state priorities, especially during phases of instability and wars.

Flawed rationale lead to flawed interventions, in other words, decisions to invest in cybersecurity ought to be on principles of insight and long-term survival.

Absence of a legal framework in relation to cyber space warfare provides attackers with a disproportionately large amount of cover and plausible deniability. Countries had questioned the

[1] https://www.controlrisks.com/our-thinking/insights/maritime-businesses-face-challenging-cyber-threats

[2] A.I in Cyber Warfare: A new Challenger in the Mediterranean Battlefields- KAS- IPASSS

fact if existing bodies of international law and military jurisdiction of space apply to cyberspace. This uncertainty is giving organized crime group, hacktivist, and nation states added flexibility that is not sustainable for the future of warfare.

The threat landscape is rapidly changing and cyber defenses policies ought to be just as robust. That being said, we are working on streamlining cyber defense procedures, methods, governance and the integration of cyber defense/offense into relevant nations operations and command control. We also have the capability to develop capacity to prepare curriculum and training exercises, encourage cooperation, and exchange of best practices and information sharing between nations. A CERT can be set up to centralize expertise, prevent, mitigate, and recover from cyber-attacks.

KAS and IPASSS can mutually organize workshops to conduct cyber defense exercises to develop multi-lateral expertise and allow nation's representative to join on a voluntary basis; a workshop that focuses on people development as much as the technology. The objective is to establish a command and control center that can support and liaise with military and intelligence officers with situation awareness and assist where required.

Recommendations

We would present some practical recommendations on how to increase cybersecurity capabilities in the Mediterranean and MENA Region:

- Strengthen cybersecurity legislation and institutional capacities.
- Ensure the appropriate balance between privacy, while at the same time protecting state institutions and critical infrastructures.
- Reassess vulnerabilities and improve national cyber infrastructures.
- Anticipate threats using machine-learning methodologies.
- Secure machine learning, especially when it comes to high-stakes applications such as national security.
- Cyber diplomacy to go hand-in-hand with building capacities of stakeholders.
- Strengthen multilateral coordination and openly communicate efforts and best practices.
- Improve and Invest in Cybersecurity (defensive and offensive) talents and higher education institutions to enable regional partnerships to meet today's human-cybersecurity skills needs; human capital is indispensable.
- Increase number of joint projects designed to respond to attacks through international cooperation, dialogue, capacity building, and joint investigations.
- At the security level, international cooperation conducted with allies, neighbors and partners, notably in terms of joint exercises and training.
- Adopt a cyber-warfare treaty, (similar to the EU cybersecurity act), with objectives to strengthen trust and enhance cooperation between Euro-Med member States, and prepare the region for the cyber challenges of tomorrow.
- Cyber-attacks know no borders. All layers of society is impacted and we need to be ready to respond to large scale and cross-border cyber-attacks and cyber crisis.
- Cross-border interdependencies means the need for effective cooperation between Euro-Med States for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).
- Exchange of a variety of cyber defense-related information and assistance to improve cyber incident prevention, resilience and response capabilities.
- Setting up a multi-agency Computer Emergency Response Teams (CERTs).
- Creation of a Cyber Defense Committee for good governance, political governance and cyber defense policy. It will include leaders of policy, military, operational and technical with responsibilities for cyber defense.

Frequent cyber threats to the security of the Mediterranean are becoming more destructive and coercive.

IPASSS and KAS will continue to adapt to the evolving cyber threat landscape and add value to nation states. We seek collective defense, crisis management and cooperative security. We need to defend our networks and operations against the growing sophistication of the cyber threats we will continue to face.

Konrad-Adenauer-Stiftung
Regional Program South Mediterranean
T +216 70 029 460
F +216 71 962 381
Info.poldimed@kas.de
www.kas.de/poldim