Commission: OSCE (Organization for Security and Co-operation in Europe Council)

Subject: Towards a strategy of cooperation between the OSCE and the European Union to counter terrorism and cyberwarfare?

Author: Germany

Germany is a key member of the European Union, an influential member of the G7, and an active participant in OSCE's activities. The Nation is a Federal Democracy ruled by its president, Frank-Walter Steinmeier, and the chancellor, Olaf Scholz. Since the Cold War began, our country had to experiment with security instabilities and the elder CSCE has helped a lot throughout the tensions, by helping with communication between the East and the West. After the end of the Cold War and fall of the Berlin Wall and Iron Curtain, Germany stayed faithful to the organization alongside 57 other participants.

Currently, cyberwarfare and terrorism have been a common issue for various Nations that fight together or against each other on that matter for several years now, and it is important to implement new strategies, especially in this period of vulnerability, in which Europe is in a great deal of tension, and where digital technology and telecommunication are everywhere, growing.

Terrorist attacks have increased over the past decades and Germany aware of the possible hacking risks that anyone may encounter at a company or personal level. As for cyberwarfare, the new technological advancements have developed a possibility to impact anyone via the internet or any telecommunication device, with the risk to get inside the personal data of any web user. As a matter of fact, Germany, with its powerful economy, is a really interconnected country to keep up with an increasingly interconnected world, which is fundamental to keep pace with the latest progresses and economic needs.

Germany firmly believes that this situation of constant threatening is fundamentally unacceptable. The collaboration between the OSCE and UE, on terrorism and cyberwarfare and this specific encounter should lead to better security management of borders and public control without forgetting the accidents. By doing so, we assure the protection and security to our populations and keep remembering the lost citizens to make sure we learn from our mistakes. To stick with this idea, every country should implement firmly the 2004 charter on preventing and combating terrorism. As for cyberwarfare, we think keeping a defensive position is the most reasonable thing to do since we can't accept attacks beforehand. We have to think in a way where we can plan preventive measures and the ability to anticipate, counter and retaliate where needed, so we can keep economic and social prosperity out of attacks reach. The Federal government walks alongside the Bundeswehr, the security-based on governmental mandates, to ensure technological liberty and data protection.

Even though the German delegation asks its fellow countries to collaborate, the state has already applied measures to solve the problems in those two domains. Foremost, the government invested a total of $255 million in programs against all types of terrorism, in which $118 million dollars have been placed for the National Prevention Strategy Against Islamist Extremism. In addition to that, laws and security border systems have been enforced to prevent the arrival of new terrorists. An important measure has been the creation of a National Remembrance Day for Victims of Terrorist Violence that was inaugurated on the last 22nd of March after the acts of violence committed in

different events such as the NSU attacks between 2000 and 2007, the Islamist attack in 2006 at the Breitscheidplatz Christmas market in Berlin, and the racist killing in 2020 in the city of Haney. The federal-state government tries to deal with the losses as well as they can, trying to be respectful and empathetic. To help the ones affected by those events, our country tries to improve the therapeutic support given to those who have suffered traumas because of the attacks.

Due to the increasing cybercrime threat, the state has taken numerous courses of action to counter the menaces. Germany invested to help the maintenance of economic and social prosperity by developing an important level of protection and resilience of our interlinked information infrastructures without hampering its use.

Moreover, there have been law enforcement measures that ensure specifically that any citizens accused of hacking or trespassing on others' personal data will receive an exceeding three years imprisonment on top of a fine. Germany has already invested in this issue in 2011 and was a major contributor with The Federal Government's Cybersecurity Strategy for Germany, where it provided a forward-looking cyber-security policy with many useful measures that are nowadays used by European countries.

Germany concludes this text of general political matter by adding that our country especially aims at ensuring the coherence and capabilities of the international community to protect the populations and cyberspace. The German delegation wants to make it clear to other nations that collaboration is fundamental to ensure safety in cyberspace and avoid economic and social tensions. Germany has hope in a future where safety will reign. We know the importance of cooperation and alongside our EU European Partners and OSCE member states we are determined to continue improving our collective defense vs terrorism and cyberwarfare.