Hybrid
Warfare
Research
Institute

Udruga Sv. Jurja
St. George Association

CONCLUSIONS OF THE 4TH ZAGREB SECURITY FORUM (2019)

RECOGNIZING AND FACING EMERGING HYBRID AND CYBER CHALLENGES – MAKING SOCIETY AND CRITICAL INFRASTRUCTURE RESILIENT

Strengthening Democracy,
Protecting Freedom and Society

Scientific, Theoretical, and Practical Approaches to Hybrid Warfare

There are three dominant approaches:

I. Scientific approaches are based on technology and the premise that better technology defeats threats. Technologies can be evolutionary (in most cases), or revolutionary. But the main problem is that even the best technologies depend on people to use them, and people are sometimes overconfident, untrained or make wrong decisions.

II. Theoretical approaches evolve around strategic and tactical concepts, maintaining that better planning means better defence.

Bar-Ilan University

The three main theoretical concepts are Deterrence, Attribution, and Retaliation.

- DETERRENCE
  Conventional deterrence is based on conventional capabilities and the will to use them. Today, much of each country`s conventional military forces are mostly irrelevant (e.g. would Britain and Spain go to a military war over the territorial water of Gibraltar?).
  How can we develop deterrence in the digital world?

Can we deter countries, organizations or individual people in the digital sphere?

- ATTRIBUTION

  In previous decades, the source of aggression, or threat thereof, was instantly recognizable. You could see who is attacking you. Today the sources cyber-attacks are well hidden and camouflaged, it also takes time to identify the sources of a threat.

  We need improved ways and means of hybrid attribution if deterrence is to be credible.

- RETALIATION

  In former days, attribution was clear, and so were the potential targets for retribution. But today, with so many different and well camouflaged cyber and hybrid threats, who do you retaliate against? The debate between defensive and offensive cyber warfare slowly becomes irrelevant, as technological capabilities merge into one-stop solutions. Does a country retaliate when the attack is aimed at an organization? Or a private individual?

Another Problem: uncertainty of capabilities on the attacking side. How to scale your retaliation to the real threat level posed by the other side. Simply said, we don't know what kind of capabilities are being developed, or even whether they are revolutionary rather than evolutionary (examples: STUXNET, FLAME, etc.)

III. Practical approaches emphasize the need for effective crisis management, the development of flexible crisis management structures and procedures. Having effective crisis management structures, which are regularly and realistically trained, means you can respond to many different threats or incidents, even very unexpected. This approach also includes the need for effective crisis communication.

Conclusions:

Problems, challenge areas, lessons learned, recommendations

1. Hybrid threats are real and present danger. Hybrid threats and crises required a hybrid response, not only technology-based but designed to make use of existing crisis management structures and people.
2. Crisis management must be planned, rehearsed and regularly trained under realistic conditions (Can you imagine a pilot learning to fly an airline from a book, without spending time in a simulator and in the air?). Simply having the right technology does not guaranty success. The human element is as important as technology.
3. International cooperation is not a luxury but an imperative. Hybrid threats are inherently global in their nature. Therefore, the response must be international as well.
4. Stand-alone solutions make cooperation difficult. So do independent units and very different organizational frameworks and cultures (especially in cyber). We need more standardization and jointly accepted certification.
5. Technological developments must place emphasis on four stages its adoption: Intercompatibility, Interoperability, Training and Certification.
6. Government entities, ministries and agencies fight for budgets and competencies in the field of hybrid warfare. In reality, 80% of security of critical infrastructures lie in the hands of private security firms. The private sector must be perceived, and treated, as at least equal partner in the development and implementation of hybrid security strategies and tactics.

7. Cross-border training should be developed in a similar way to existing interstate catastrophe training already in place.
8. Hybrid threats in form of influence operations to democratic society, especially in the domain of malicious election influence, needs development of social resilience. Social resilience should be based on individual and different group approaches by academic, state, public and private sector activities.
9. In order to be effective, disinformation campaigns need time and preparations. As mentioned in points 3 and 6, positive influence of cooperation between them in developing effective and reliable artificial intelligence and social network tools (AIT and SNT), should be key activity that can help to recognise and attribute hybrid threats in their early phase. AIT and SNT, supported with national and international security structure, should be developed as an early warning system.
10. Joint activities of academic, state, public and private sector at national and international level, on development of information and digital literacy and critical thinking is precondition for information and digital sovereignty, on national and international level. Aim is to preserve and further positive development of present levels of democracy and freedoms of individuals and societies.
11. It is necessary to develop internationally validated and accepted rules/convention of engagement in hybrid activities that are going to be possible to apply and to enforce their adoption and respect. Hybrid attacks on critical infrastructures should be treated as a use of WMD.

SAPERE AUDE · CROATIA · IIHS

Hybrid
Warfare
Research
Institute

Udruga Sv. Jurja
St. George Association

Zagreb 5ecurity Forum 2020

Zagreb, March 13-14, 2020

NATO OTAN *This workshop is supported by:* The NATO Science for Peace and Security Programme

SAPERE AUDE · CROATIA · IIHS

Hybrid
Warfare
Research
Institute

Udruga Sv. Jurja
St. George Association

4th Zagreb Security Forum was supported by:

HEP d.d.

JANAF

KONRAD ADENAUER STIFTUNG

institut.hr
za elektroničko poslovanje

INFODOM

ITAS PRVOMAJSKA

Večernji list

NACIONAL

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Institut za istraživanje hibridnih sukoba, Teslina 10, Zagreb; OIB: 31073348655,
IBAN: HR35 2390 0011 1009 9221 2, Hrvatska poštanska banka, Zagreb
www.zagrebsecurityforum.com