EU and Cyberterrorism. Added Value or Chimera?

Filippo Pierozzi

Introduction

Whilst the famous claim that "cyber war will not take place"[1] may leave room for and policy-makers' debates, it is common consensus that -despite the mediatic and security communities' hype[2] - "there has not been so far a single recorded instance of cyber-terrorism"[3]

Accordingly, in assessing the European's Union added value to EU crisis management in cyberterrorism both for the EU and for its member states, utmost attention will be paid to carefully define the scope of our inquiry.

In fact, 'cyberterrorism' in the EU policy environment may be deem a misnomer since it has not been yet explicitly defined at EU level.[4] While 'cyber-attacks' represent the main focus of a wide range of EU policy measures, 'cyber-terrorism' has not been much of a concern[5] and it is broadly understood as a potential component of the overall threat environment emerging from cyberspace.[6]

---

[1] T. Rid, "Cyber war will not take place", *Journal of strategic studies*, *35*(1), 2014, pp.5-32.

[2] See, e.g. L. Jarvis, Macdonald, S., & Whiting, A., "Unpacking cyberterrorism discourse", *European Journal of International Security*, *2*(1), 2017, pp.64-87

[3] J. Argomaniz, Bures, O., & Kaunert, C., *EU counter-terrorism and intelligence: A critical assessment*, London, Routledge, 2016, p.80.

[4] CyberRoad, "Cyberterrorism. Stakeholder Needs and Threats Evaluation, European Commission Seventh Framework Programme, 2016, p.17, retrieved 15 March 2018: https://www.cyberroad-project.eu/m/filer_public/2016/05/02/d61_cyber_terrorism_stakeholder_needs_and_threats_evaluation.pdf

[5] J. Argomaniz, "European Union responses to terrorist use of the Internet". *Cooperation and Conflict*, *50*(2), 2015, pp.250-268, 255.

[6] W. Rohrig & Llopis, S., "Cyberterrorism: A Challenge for External and Internal Security" in M. Conway et al.(Eds.), *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam, IOS Press, 2017, p.25.

1. Cyberterrorism in the Framework of EU Cyber Crises Management

As suggested by the EU Agency for Network and Information Security (ENISA), while a 'cyber crisis' may be an oxymoron, the combination of the two terms is highly significant.[7] Therefore, to fully grasp the actual and prospective value EU action and to cope with inherently transboundary crises,[8] the 'cybersecurity' dimension should be mainstreamed in all policy areas[9] and embedded in the crisis management cycle.
, "Taking hint from EU Commission's CyberRoad Project, cyberterrorism may be better defined as comprising "unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government of its people in furtherance of political or social objectives."[10] *Condicio sine qua non* of 'cyberterrorism' being both the intent and the effective result in "violence against persons or property or enough harm to generate fear".[11]

When evaluating EU preparedness, it is noteworthy emphasizing that whilst "crisis management at EU-level still lacks the proper mechanism to support effectively the EU-wide cybersecurity community in the event of a cyber crisis,[12] nonetheless EU-driven cooperation between member states is emerging. In this regard, "EU can provide a strong *added value* in supporting the cooperation between member states."[13] Individual states' capabilities may benefit from the enhancement of ENISA capacities and its contribution to spread best practices and assisting in the development of national contingency plans. However, a thorough assessment of potential benefits at the Union scale has to address the crisis management takeaways from the first and most serious cyber

---

[7] P. Trimintzios et al., *Common practices of EU-level crisis management and applicability to cyber crises*, ENISA, 2015, p.23.

[8] Characterized by the involvement of multiple jurisdictions, the undermining of various policy sectors and the swift escalating dynamic.: C. Ansell, Boin, A., & Keller, A., "Managing transboundary crises: Identifying the building blocks of an effective response system". *Journal of Contingencies and Crisis Management*, *18*(4), 2010, 195-207, p.195.

[9] European Union Global Strategy, Cyber-Security, retrieved 16 March 2018: https://europa.eu/globalstrategy/en/cyber-security

[10] Denning, D.E., "Cyberterrorism", Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. *Focus on Terrorism*, *9*.

[11] Denning, *op. cit.*

[12] Trimintzios et al., *Report on Cyber Crisis Cooperation and Management*, ENISA, 2015, p.4.

[13] Council of the European Union, Council Conclusions "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", Brussels, 20 November 2017, p.5.

incident EU has faced so far: Estonia 2007 Distributed Denial of Service attacks.[14] It is good to note that, after ten years, the way the EU responded remains a precious benchmark to assess the actual and potential benefits of a far-reaching cyber crisis management approach for member states and its potential impact on the EU as a whole.

2. The Significance of a Common Lexicon in Cyber Crises Management

An accurate definition of 'cyberterrorism', far from being a mundane theoretical exercise, is particularly relevant for understanding the range of crisis management tools at the EU disposal. In fact, including the "terrorist use of computers as a facilitator"[15] or 'cyberattacks perpetrated by terrorists'[16] within the scope of 'cyberterrorism' swallows up the whole phenomenon as an incidental section of EU counter-terrorism policies. Following this line of argument, a 2011 European Parliament Report underlined how "in recent decades terrorism has taken new forms such as cyber-terrorism".[17]

However, situating potential cyberterrorist attacks in the sole domain of 'counter-terrorism policies' could hamper EU responsiveness by further jeopardizing a highly fragmented policy field, where a unique approach linking risk to terrorism is still missing.[18] Furthermore, beyond the transboundary nature of potential cyber-crises triggered by cyberterrorist attacks, the digital component adds another layer of complexity.[19] In fact, while "the severity of a crisis tends to be measured by the severity of its impacts",[20] the lack of a cyber sector *per se* challenges the traditional priority given to impacts.

---

[14] See E. Tikk-Ringas, Kaska, K. & Vihul L., *International Cyber Incidents: Legal Considerations*, CCDCOE, Tallinn, 2010.

[15] M. Conway "Cyberterrorism: media myth or clear and present danger?" in J. Irwin(Ed.) *War and virtual war: the challenges to communities.* Amsterdam, Rodopi, 2004, p.88.

[16] CyberRoad, *op. cit.*, p.18.

[17] European Parliament, *Resolution on EU counter-terrorism policy: main achievements and future challenges*, 14 December 2011, 2010/2311(INI).

[18] J. Wouters & Sanderijn, D., "Managing the Unmanageable: The European Union and Terrorism", in H. Micklitz & Tridimas T., *Risk and EU Law*, Cheltenham, Edgar Publishing, 2015, p.95.

[19] The inherently aterritorial nature of cyberspace further complicate the transboundary nature of digital disruptions. See J.P. Barlow, *Declaration of Independence for Cyberspace*, 9 February 1996, Retrieved 23 March 2018: https://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html

[20] Trimintzios et al., *op. cit.*, p.5.

Furthermore, the cyber crises driven by terrorist intents urge for a paradigm shift to a "combined management of impacts and causes".[21] Therefore, a collective response pursued through the "coordination with other crisis management mechanisms at EU, national and sectoral level"[22] would constitute the preferred solution to manage perspective cyberterrorist interferences.

The EU preparedness may benefit from the establishment of a set of common principles contributing to ensure "consistency of approach and harmonisation of definitions".[23]

3. An Events-Triggered Development

As argued in the preamble, the development of nascent EU capacity in the field of cyber-crisis management would not have been possible without the post-Estonian lesson learning. The 2007 attacks triggered a reconstruction of roles and sense making among the key stakeholders and institutions as well as 'organizational readjustment'.[24] At the time - as vocally denounced by then-Estonian President - the EU legislation on cybersecurity and cyberterrorism was "dangerously and unaccountably deficient."[25]

While ENISA was already established and functioning as an information hub tasked with providing support to individual member states,[26] the overall EU response lacked a timely intervention both at the strategic and operational level. It failed to deliver a tangible response: the cooperative efforts remained at the bilateral level on voluntary basis with the computer emergency response teams (CERTs) of Finland, Germany and Slovenia providing contacts and technical assistance.[27]

ENISA – despite its crucial role in EU cyber crisis management – did not add to member states' capacities. Indeed, the real added value of ENISA should lies in its ability to

---

[21] *Ibid.*

[22] European Commission, Annex I ANNEX to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C (2017) 6100, 13 September 2017, p.1.

[23] Trimintzios et al., *op. cit.*, p.14.

[24] M. Pearson & Clair J. "Reframing Crisis Management" in Boin, A. (Ed.) *Crisis Management*, London, SAGE, 2008, p.11.

[25] Office of the President of the Republic of Estonia (2007) President of the Republic On Victory Day, Rapla, 23 June 2007, retrieved 21 March 2018: https://vp2006-2016.president.ee/en/official-duties/speeches/2584-president-of-the-republic-on-victory-day-23-june-2007-in-rapla/

[26] A. Fritzon et al. "Protecting Europe's critical infrastructures: problems and prospects". *Journal of Contingencies and Crisis Management*, *15*(1), 2007, 30-41, p.34.

[27] A. Schmidt, "The Estonian Cyberattacks", in Healey, J. (Ed.) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Washington, Cyber Conflict Studies Association, 2013, p.13.

enhance cooperation between both member states and information security communities.[28] While still suffering from a "largely technical, engineering-driven governance system' between various national teams"[29], the EU cyber crisis management apparatus over time has been able to develop a distinctive identity.
Not limiting cyberterrorism to a branch of counter-terrorism, the EU will be able to retain response flexibility and to rely on an adaptable and scalable network to cope with cyberterrorist attacks. Coherently, EU officials warned of the potential effectiveness costs of both conferring a 'cyberterrorism' portfolio to the EU counter-terrorism coordinator or creating a 'EU cybersecurity crisis management coordinator.[30]

4. Disentangling EU Added Value: The Potential for a Scaled-Up Response

ENISA constitutes the focal point in EU cyber crisis management as an information-sharing hub.[31] While ENISA contributes as a 'capacity builder' for member states acting as the Secretariat of the EU CSIRT network created by the NIS Directive[32] , it is also crucial as a source of independent advice and guidance and as a partner in policy-implementation support.[33] Overall, EU major contributions to member states' capacities pertain to standard-setting, information sharing and streamlining best practices.[34]
In this regard, we argue that if 'cyberterrorism' would been included in EU lexicon this would have tangible crises management effect enabling a more coordinated approach and common understanding of the events the Union is facing.[35]
The EU contribution to the Europe-as-a-whole may be fully appreciated in the speculative scenario of a cyberterrorist attack: the potential activation of the 'solidarity clause', ex art.

---

[28] European Commission, Commission Staff Working Document on the evaluation of the European Union Agency for Network and Information Security (ENISA), SWD (2017) 502 final, 13 September 2017, p.17.
[29] J. Ruohonen, Hyrynsalmi, S., & Leppänen, V. "An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly*, *33*(4), 2016, pp. 746-756.
[30] Interview with Steve Purser, Head of ENISA Core Operations, Paris, 28 March 2017.
[31] ENISA, Strategies for Incident Response and Cyber Crisis Cooperation, 2016, p.24.
[32] *Ibid.*, p.18.
[33] European Commission, *op. cit.*, 2017.
[34] Cfr. ENISA, *ENISA Programming Document 2018-2020*, January 2017, retrieved 13 March 2018: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202017_1%20SPD2018_2020%20Draft.pdf
[35] A sharp difference may be witnessed in the 2007 Estonian attack where the lack of common sense making further weakened the scarcely developed policy framework; see, e.g. S. Herzog, S., "Revisiting the Estonian cyber attacks: Digital threats and multinational responses", *Journal of Strategic Security*, N. 2 Vol. 4, 2011, pp.49-60.

222 TFEU, would constitute a qualitative step forward in EU added-value to Union's resilience facing cyber-attacks.

Moreover, while the boundaries of what falls within 'cyberterrorism' are still blurred, the EU opted for a wide scope of applicability for the 'Solidarity Clause'[36]: in fact, the Solidarity Clause may be activated "in order to address the consequences of a severe cyber-attack dealing with the consequences of which would be beyond the capacities of a Member State".[37] Its potential activation should be "an integral part of permanent EU crisis response and crisis management" able to fully exploit the existing sectoral policies and capabilities.[38]

EU was led by an increased awareness of the "interconnectedness between the Member States and their inherent limitations to tackle a complex disaster provoked by a cyber-attack"[39] thus requiring a whole-of-EU approach.

The potential threat of politically-motivated cyber-attacks, led the EP to boost EU crisis management capabilities recognising that "[…]cyberattacks against critical infrastructure, that are launched with the aim of causing severe damage and disruption to a Member State […] may also trigger the Mutual Defence Clause"[40] (art. 42.7 TEU). Here, the EP went beyond traditional international law consensus that - given the reference in art. 42.7 TFEU to 'armed aggression' – may rule out certain cyber-attacks.[41]

Nevertheless, the decision to activate the clauses is a political rather than a technical one:[42] accordingly, the potential benefits for the EU in the case of a cyberterrorist attack still rest on member states' discretion and political considerations.

---

[36] CCDCOE, "EU solidarity clause and cyber disaster", 19 November 2014, retrieved 20 March 2018: https://ccdcoe.org/EU%20Solidarity%20Clause%20and%20Cyber%20Disaster.html

[37] Council of the European Union, Council Decision on the arrangements for the implementation by the Union of the solidarity clause, 24 June 2014, 2014/415/EU.

[38] I. Govaere & Poli, S. (Eds.), *EU management of global emergencies: legal framework for combating threats and crises*, Leiden, Martinus Nijhoff Publishers, 2014, p.125.

[39] European Parliament, "Cybersecurity and cyberdefence", June 2015, p.1. retrieved 14 March 2018: http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI%282015%29559488_EN.pdf

[40] *Ibid.*

[41] N. Tsagourias, & Buchan, R. (Eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham. Edward Elgar Publishing, 2015, p.418.

[42] Interview with EU Official on EU Digital Policies, Brussels, 19 February 2017.

5. Mainstreaming 'Cyber' in Crisis Management

The need for an all-encompassing EU cyber crisis management is a pressing issue: while cyber-attacks are inherently a cross-border phenomenon, policy responses are predominantly national.[43]

Prospective cyberterrorist attacks call for a Copernican revolution in crises' assessment: "when a cyber-attack takes place, a fast and effective response can mitigate its impact". Therefore, we argue that the cyber aspects should be mainstreamed into existing EU crisis management mechanisms.[44]

Nonetheless, EU lacked a wide-ranging approach to tackle cyberterrorism.[45] While the EU has stepped up its efforts to face the terrorist use of the internet, cyberterrorism is considered as a threat with a "high potential, but low probability"[46] and therefore not enshrined in crisis management mechanisms. Finally, the proposal of a cybersecurity coordinator for cyber crisis management has not been followed through. Introducing new institutional players without enhancing complementarity and network responses may render even more tangled the EU crisis management scenario.

Policy Recommendations

Reconciling the 'cyber' with the 'terrorism' facet of our inquiry, we reiterate ENISA's takeaway from EU counter-terrorism policies. Facing inherently trans-sectoral and trans-boundary crises provoked by terrorist attacks perpetrated against and through digital means, the EU should aim at establishing common principles underpinning legislative measures created "consistency of approach and harmonisation of definitions, which in turn contributed to achieving a higher level of preparedness"[47].

Furthermore, "the cyber aspects should be mainstreamed into existing EU crisis management mechanisms".[48] Accordingly, the EU added value in countering

---

[43] European Commission, Proposal for a Regulation of The European Parliament and of the Council on ENISA, Brussels, 13 September 2017, 2017/0225, p.23.

[44] European Commission, Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", Brussels, 13 September 2017, pp.7-8.

[45] European Parliamentary Research Service, Cyber security in the European Union, 12 November 2013, p.4

[46] EUROPOL, *Terrorism Situation and Threat Report,* The Hague, 2016, p.17.

[47] P. Trimintzios et al, *op. cit.*, p.14.

[48] European Commission, *op. cit.*

cyberterrorism should start in defining the boundaries of the concept and complementing in a functional manner member states' effort.

Bibliography

Ansell, Chris, Arjen Boin & Ann Keller "Managing transboundary crises: Identifying the building blocks of an effective response system". *Journal of Contingencies and Crisis Management*, 18.4, 2010, pp. 195-207.

Argomaniz, Javier, "European Union responses to terrorist use of the Internet". *Cooperation and Conflict*, 50 (2), 2015, pp.250-268.

Argomaniz, Javier; Bures, Oldrich; Kaunert, Christian (ed.). *EU Counter-terrorism and Intelligence: A Critical Assessment*, London, Routledge, 2017.

Barlow, John Perry, *Declaration of Independence for Cyberspace*, 9 February 1996, Retrieved 23 March 2018: https://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html

CCDCOE, "EU solidarity clause and cyber disaster", 19 November 2014, retrieved 20 March 2018: https://ccdcoe.org/EU%20Solidarity%20Clause%20and%20Cyber%20Disaster.html

Conway, Maura "Cyberterrorism: media myth or clear and present danger?" in Irwin, Jones (Ed.) *War and virtual war: the challenges to communities.* Amsterdam, Rodopi, 2004.

Denning, Dorothy E., "Cyberterrorism", Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. *Focus on Terrorism*, 9, 2000.

Fritzon, Åsa, et al. "Protecting Europe's critical infrastructures: problems and prospects", *Journal of Contingencies and Crisis Management*, 15(1), 2007, pp. 30-41.

Govaere, Inge & Sara Poli (Eds.), *EU management of global emergencies: legal framework for combating threats and crises*, Leiden, Martinus Nijhoff Publishers, 2014.

Herzog, Stephen, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses", *Journal of Strategic Security*, N. 2 Vol. 4, 2011, pp.49-60.

Jarvis, Lee; Stuart Macdonald & Andrew Whiting "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat", *European Journal of International Security*, 2(1), 2017, pp. 64-87.

Pearson, Christine M. & Judith Clair, "Reframing Crisis Management" in Boin, Arjen (Ed.) *Crisis Management,* London, SAGE, 2008.

Rid, Thomas "Cyber war will not take place", *Journal of strategic studies*, *35*(1), 2014, pp.5-32.

Rohrig, Wolfgang & Salvador, Llopis, "Cyberterrorism: A Challenge for External and Internal Security" in M. Conway et al.(Eds.), *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam, IOS Press, 2017.

Ruohonen, Jukka; Sami Hyrynsalmi & Ville Leppänen "An outlook on the institutional evolution of the European Union cyber security apparatus", *Government Information Quarterly*, 33(4), 2016, pp. 746-756.

Schmidt, Andreas. "The Estonian Cyberattacks", in Healey, J. (Ed.) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* Washington, Cyber Conflict Studies Association, 2013,

Tikk-Ringas, Eneken; Kadri Kaska & Liis Vihul, *International cyber incidents: Legal considerations*, Tallinn, Cooperative Cyber Defence Centre of Excellence, 2010.

Tsagourias, Nicholas & Russell, Buchan (Eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham. Edward Elgar Publishing, 2015.

Wouters, Jan & Duquet, Sanderijn,"Managing the Unmanageable: The European Union and Terrorism", in Micklitz, Hans & Takis, Tridimas, *Risk and EU Law*, Cheltenham, Edgar Publishing, 2015

Documents and Additional Sources

ENISA, Strategies for Incident Response and Cyber Crisis Cooperation, 2016, retrieved 22 March 2018: https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

ENISA, *ENISA Programming Document 2018-2020*, January 2017, retrieved 13 March 2018: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202017_1%20SPD2018_2020%20Draft.pdf

European Commission, Commission Staff Working Document on the evaluation of the European Union Agency for Network and Information Security (ENISA), SWD (2017) 502 final, 13 September 2017.

EUROPOL, *Terrorism Situation and Threat Report,* The Hague, 2016.

Interview with EU Official on EU Digital Policies, Brussels, 19 February 2017.

Interview with Steve Purser, Head of ENISA Core Operations, Paris, 28 March 2017.