

	Friday July 3rd	Monday July 6th	Tuesday July 7th	Wednesday July 8th	Thursday July 9th	Friday July 10th				
10:00 - 10:20 <sup>†</sup> 11:00 - 11:20 <sup>†</sup> 12:00 - 12:20 <sup>‡</sup>	Opening chat/ morning coffee (optional)									
10:20 - 10:30 * 11:20 - 11:30 † 12:20 - 12:30 ‡	Morning check-in, including a discussion about the day's readings and content									
10:30 - 12:00 * 11:30 - 13:00 † 12:30 - 14:00 ‡	Lecture on the Digital Transatlantic rift	Lecture on Social Media moderation and Big Tech	Lecture on geolocation and open source investigations	Lecture on investigative journalism	Lecture on disinformation and election security	Lecture on digital security				
	with Peter Chase	with Jillian C York	with Myriam Redondo	with Rana Sabbagh	with Nad'a Kovalčíková	with Łukasz Król				
12:00 - 13:30 <sup>*</sup> 13:00 - 14:30 <sup>†</sup> 14:00 - 15:30 <sup>‡</sup>	Lunch break, away from computers									
13:30 - 15:00 * 14:30 - 16:00 † 15:30 - 17:00 ‡	Discussion on data privacy, GDPR, and third countries	Workshop on Social Media moderation and Big Tech	Workshop on geolocation and open source investigations	Workshop on investigative journalism	Workshop on disinformation and election security	Discussion on digital security				













<sup>\*</sup> Warsaw, Belgrade, Podgorica, Pristina, Sarajevo, Skopje, Tirana

<sup>†</sup> Chisinau, Kyiv, Minsk

<sup>‡</sup> Baku, Tbilisi, Yerevan



Introduction: The digital transatlantic rift	Day one: Social Media moderation and Big Tech	Day two: Geolocation and open source investigations	Day three: Investigative journalism	Day four: Disinformation and election security	Day five: Digital security
Peter Chase	Jillian C York	Myriam Redondo	Rana Sabbagh	Dr Nad'a Kovalčíková	Łukasz Król
Senior Fellow, GMF Brussels, specialising in digital affairs and transatlantic relations	Director for International Freedom of Expression at the Electronic Frontier Foundation	Journalist and trainer currently working as journalist for Verifica RTVE and as associate lecturer for Complutense University	Senior Editor, Middle East/ North Africa, OCCRP	Program Manager and Fellow at the Alliance for Securing Democracy (ASD), GMF	Digital Projects Coordinator a the College of Europe in Natolin, digital security traine
(bio)	(bio)	(bio)	<u>(bio)</u>	<u>(bio)</u>	(bio)
This section will look at how the EU and US approach big tech regulation, where they agree and where they differ. It would also investigate how this complex transatlantic relationship and debate shape the fight against disinformation in the Eastern Partnership and the Western Balkans.	All online platforms need to decide whether to remove or downrank undesirable or offensive content. Still, the criteria they use to make this decision can often seem undemocratic or arbitrary. This session will look at what types of content are removed and what stays up online, and how big tech firms face an uncomfortable paradox in that they host public speech on private infrastructure	Based on very popular WEASA courses offered by trainers from institutions such as DW or Bellingcat, this session will teach participants how to investigate crime, military movements, and corruption by using open data, such as satellite imagery, social media feeds, and publicly available databases.	This session, modelled in part on other investigative trainings that took place at Natolin, will show participants how investigative journalism functions, what information and sources it relies on, and the storytelling structures it uses. It will consist of both an in depth look at investigative techniques and a wider discussion on the social impact investigative journalism has.	This day will focus on disinformation and foreign interference more broadly, and how best to address efforts which aim to undermine democracy. It will also look at the steps that the EU, NATO, national governments and others are taking to ensure the security and integrity of elections and of other democratic processes and institutions.	This training will teach participants what steps they can take to secure their own data and communications from hostile actors. It will include modules on encrypted messaging, secure communication practices, and digital hygiene.











