Comment on the cyberattribution case study in Easter Europe.

The cybercrime attribution case study on eastern Europe tries to identify if the main origin of phishing attacks is Eastern Europe instead of China, or the U.S. That is, the researchers assert that organized crime groups from Eastern Europe are significantly involved in phishing and related cybercrime. They believe that Eastern Europeans, ’ particularly Russians and Ukrainians, play a critical role in the cybercrime world. To test this hypothesis, the study primarily focused on Australia since it was the first victim of Phishing attacks that targeted online banks. Additionally, a survey composed of individuals from Eastern Europe that have been charged with related crimes or unsolved cases where there is some connection to Eastern Europe was considered when conducting the study.

After analyzing data from various sources, the researchers conclude that the information they gathered, in conjunction with the surveys and other supporting materials, indeed highlights that Eastern European individuals and organized groups play a significant role in phishing and other related cybercrimes. They believe that the root cause for the attacks lies in an excellent technical education, criminal gangs, and economic uncertainty.

That being said, to comment on the article, the main origin of cybercrimes today is nation-states such as China, Russia, Iran, and the U.S. They are believed to be the cyberwar superpowers due to their most developed cyber warfare capabilities. As a result, most States funded cyber-attacks (conducted either by individuals or organized groups) utilize various means, including phishing to cause damage. They continue to be a primary concern. In fact, it is a growing concern of business and the community in general. Hence, it is fair to say that solely focusing on Eastern Europe as the primary origin of phishing attacks and related cybercrime is an outdated assertion that can have an inconclusive explanation.