Korzystne warunki dla takiego scenariusza działań hybrydowych wynikały z infrastruktury teleinformatycznej Gruzji. Prawie połowa z trzynastu połączeń do Internetu przebiegała przez Rosję. Sytuacja jednak się zmieniła. Jak podał w czasie spotkania w Georgian Foundation for Strategic and International Studies, podczas wystąpienia na temat "State-sponsored Cyber Terrorism: Georgia's Experience." K. Mshvidobadze: „Po 2008 roku kabel światłowodowy Poti (Batumi) – Varna „Kaukaz" obsługuje ok. 90% gruzińskiego Internetu[36]".

Gruzja prześledziła drogę skierowanych przeciwko niej cyberdziałań i nie ma wątpliwości, że cyberataki na nią przeprowadziła Rosja. Niestety nie mogła przypisać ich do swojego rządu.

## DZIAŁANIA NA UKRAINIE – STUDIUM PRZYPADKU

Proces poznawczy uwidocznił, że trzecim wyrazistym przykładem wykorzystania cyberprzestrzeni w działaniach hybrydowych jest konflikt na Ukrainie w 2013 roku. Jest on szeroko opisany w piśmiennictwie.

„Wojna w Donbasie (konflikt na wschodniej Ukrainie) to wojna hybrydowa na terenie obwodów donieckiego i ługańskiego Ukrainy, rozpoczęta w kwietniu 2014. Zbrojne wystąpienie separatystów (wspieranych przez rosyjską armię i siły specjalne) dążących do oderwania tego terytorium od Ukrainy było poprzedzone przez marcowe wystąpienia prorosyjskie i kryzys krymski, które nastąpiły po rewolucji Euromajdanu"[37]. Natomiast Kryzys krymski to „kryzys polityczny zapoczątkowany w 2014 roku na Półwyspie Krymskim na Ukrainie, będący efektem rewolucji Euromajdanu w tym kraju oraz interwencji wojskowej Rosji"[38].

Jednak szczegółowa analiza wydarzeń (w kontekście działań w cyberprzestrzeni) z tamtego czasu wydaje się przeczyć tym informacjom, szczególnie datowania początku konfliktu. Powyższe opisy wydają się pomijać aspekt, którego nie powinno się pomijać – działania w cyberprzestrzeni. Według Glib Pakharenko cyberataki na Ukrainę rozpoczęły się 2 grudnia 2013 roku, kiedy stało się oczywiste, że protestujący nie zamierzają opuścić Majdanu. Cyberataki typu DDoS skierowane zostały na strony internetowe opozycji, większość z nich pochodziła z komercyjnych botnetów wykorzystujących oprogramowanie złośliwe BlackEnergy and Dirt Jumper[39]. Oś czasową hybrydowego konfliktu ukraińsko-rosyjskiego przedstawiono na oryginalnych rysunkach 1.1. i 1.2.

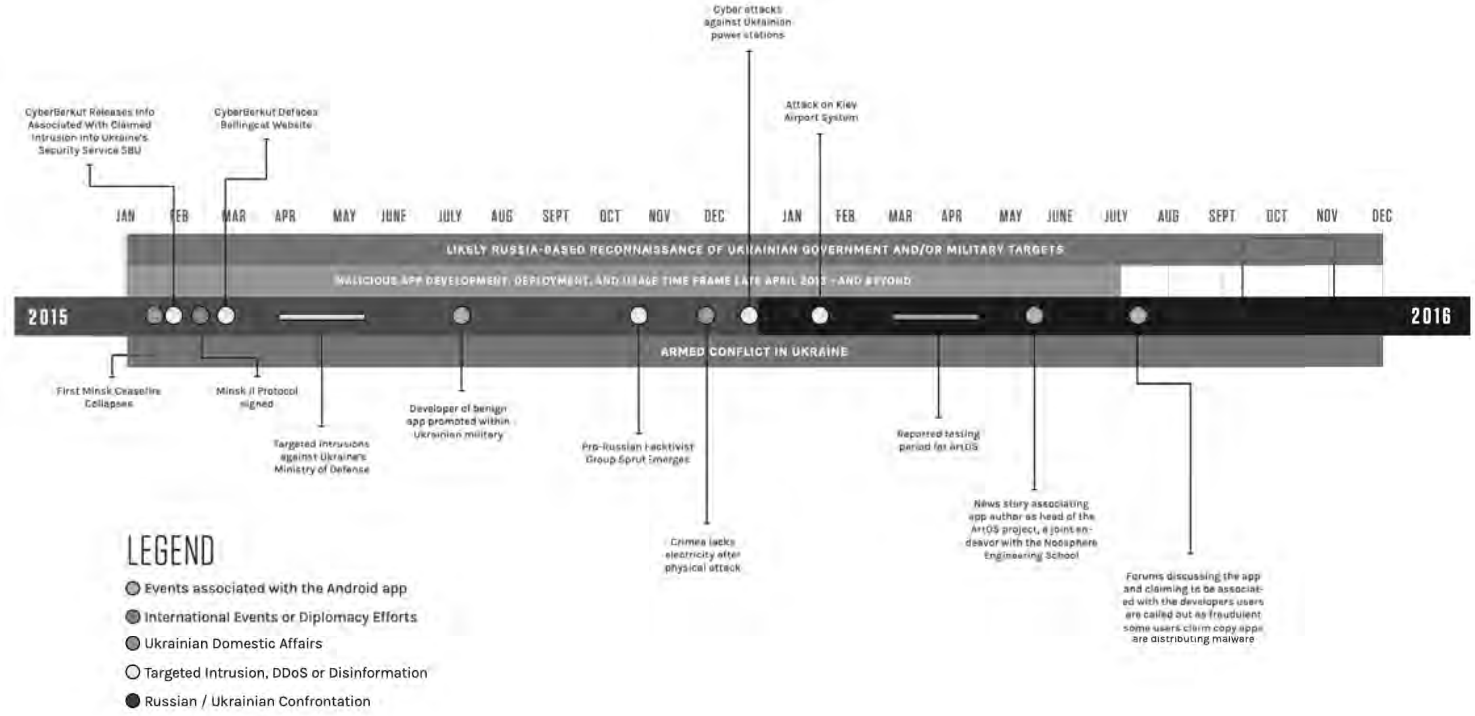
---

[36] https://gfsis.org/media/download/GSAC/cyberwar/State-sponsored_Cyber_Terrorism.pdf, Dostęp: 20.07.2018 r.

[37] R. Janczewski, *Cyberprzestrzeń – część teatru działań hybrydowych*, Przegląd Sił Zbrojnych, 2/2019, s. 41.

[38] Tamże.

[39] G. Pakharenko, *Cyber Operations at Maidan: A First-Hand Account*, [w] K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015, pp. 59–66.




**RYSUNEK 1.1.**
Oś czasowa hybrydowego konfliktu ukraińsko-gruzińskiego cz. 1

Źródło: *Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units*. Crowdstrike Global Intelligence Team, December 22, 2016. Pp. 11.