Ukraine: A Cyber Safe Haven?

by
Nadiya Kostyuk

Chapter 13 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 13, University of Michigan doctoral student Nadiya Kostyuk reviews Ukraine's cyber security policy – past, present, and future. She analyses numerous historical factors that make Ukraine a cyber safe haven: a strong science, technology, engineering, and mathematics (STEM) education, underwhelming economic performance since the fall of the Soviet Union in 1991, and social norms which dictate that stealing from the West is not a bad thing. The icing on the cake is that there are currently few cyber security regulations in Ukraine. All of these factors shed light on the vexing challenge of containing cyber crime in the region. Looking toward the future, Nadiya Kostyuk argues that Ukraine's political, military, and economic crises will inhibit the stabilisation of Ukrainian cyberspace for some time.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Ukraine: A Cyber Safe Haven?

Nadiya Kostyuk
University of Michigan

1 Introduction

Since the end of the Cold War, there has been a proliferation in online criminal activity in Eastern Europe, and Ukraine is no exception. Famous for its hacker community, Ukraine ranks among the Top 10 countries in the world in cyber crime[1] and number 15 as a source of Distributed Denial of Service (DDoS) attacks.[2] In 2012, five Ukrainian nationals stole more than $72 million from U.S. bank accounts;[3] in 2013, Ukrainian hackers stole 40 million sets of debit and credit card details from the US retail chain Target;[4] in 2014, the RAND Corporation wrote that Russian and Ukrainian (the primary language of Ukraine) were the lingua franca of online hacker forums.[5] In this light, it is natural to wonder if Ukraine is today a safe haven for cyber criminals.

To be sure, there have been some law enforcement successes, such as when numerous European countries and Europol (with the aid of the Ukrainian government) arrested five hackers who stole at least €2 million from banks all around the world.[6] However, there are major countervailing factors at play in Ukraine, which include ongoing political, military, and economic crises and the absence of *zhyvoii*

1 Victor Zhora, e-mail to the author, July 30, 2015.
2 'Украина вошла в рейтинг стран с наибольшим количеством DDoS-атак.' Minfin, June 8, 2015.http://minfin.com.ua/2015/06/08/7407564/.
3 Taylor Armerding. 'Ukraine Seen as a Growing 'haven for Hackers' March 13, 2012. http://www.csoonline.com/article/2131155/network-security/ukraine-seen-as-a-growing--haven-for-hackers-.html.
4 Charles Riley and Jose Pagliery. 'Target Will Pay Hack Victims $10 Million.' CNNMoney. March 19, 2015. http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/.
5 Lillian Ablon, Martin C. Libicki, and Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Rand Corporation, 2014.
6 Supra, note 4.

potreby (urgent need),[7] which together provide little hope that Ukraine will be able to climb down from its perch atop the world's cyber crime ladder in the near future.

In many ways, Ukraine is a perfect case study to examine the vexing dynamics of cyber crime. Its government has few cyber security regulations, its society is home to talented computer programmers, and its economy is struggling. This chapter begins with a brief description of Ukraine's current cyber crisis, to include the primary reasons why cyber crime flourishes there. Next, it discusses the future of the region based on interviews with Ukrainian and Western cybersecurity experts from public and private sectors and academia. Finally, the chapter ends with recommendations based on best practices in cyber security – all of which can help Kyiv to improve its cyber security posture. Beyond Ukraine, these insights can be applied to numerous other countries in the region.

In many ways, Ukraine is a perfect case study to examine the vexing dynamics of cyber crime.

2 Ukraine as a Cyber Safe Haven

Once the internet conquered post-Soviet daily life, many talented computer programmers who had already dabbled in illegal activities such as stealing music and movies realised that they could make a living as professional hackers. There were few cyber security regulations in Ukraine and so, as in so many other countries, cyber crime quickly evolved from a mischievous hobby to a lucrative occupation.[8]

Several factors contributed to making Ukraine a cyber safe haven. First, its Soviet school STEM (science, technology, engineering, and mathematics) education is among the best in the world. Second, its underwhelming economic performance since independence in 1991 has led these STEM specialists to explore alternative career paths, often online. Third, Ukraine's social and cultural norms dictate that stealing from the West is not always a bad thing. This factor is compounded by the relatively impersonal nature of cyberspace.[9]

At the policy level, 'cyber crimes' such as stealing intellectual property and copyright infringement were not even considered illegal in Ukraine until recently. For instance, the popular Russian social media website *vkontakte.ru* used to be a source of large-scale music and movie piracy.[10] Ukraine recently has begun to develop a common lexicon on cyber security (a pre-requisite for progress in this

7 Vlad Styran, Skype interview, July 6, 2015.
8 Supra, note 5.
9 The author can testify through personal experience.
10 Kathryn Dowling. 'VKontakte Case Puts Russian Music Piracy into Spotlight.' August 11, 2014. http://www.bbc.com/news/business-28739602.

new domain),[11] but the multiple cyber units within the Ukrainian government[12] still tend to operate independently, and rarely collaborate.[13] Moreover, as in other Eastern European countries, government employees are poorly paid and lack resources, which in turn motivates skilled specialists to leave for the private sector. Finally, due to the high level of corruption in Ukraine, even when a cyber criminal is caught, he or she can usually bribe an official to have the charges reduced or dropped.[14]

3 Ukraine as a Cyber Target

Even though Ukraine is not a rich country and is relatively new to online banking, its enterprises nonetheless lost ₴65 million[15] to cybercrime in 2014.[16] The origin of these attacks is unclear, but numerous interviewees agreed that the cyber criminals were not physically located in Ukraine. Most likely, they would follow the hacker's first '*zapovid*" ('commandment'), the so-called 'gypsy' rule: '*tam de zhyvesh, tam ne kradesh*' ('you do not steal in the place where you live').[17] When asked whether Russia could be a source of such attacks, Vlad Styran, an information security consultant at Berezha Security, answered affirmatively, but explained that some groups originally operating from Russia have moved to Ukraine, mostly to the self-proclaimed Donetsk National Republic (DNR) and the Luhansk National Republic (LNR).[18] However, these groups may not be attacking Ukraine directly, but Western countries farther afield, similar to online criminals in Romania, Turkey, and Belarus.[19] In Ukraine, the domestic climate, technical capabilities, and resources are better suited to criminals who engage in credit card fraud,[20] and as long as they steal money in small amounts, no one will touch them.[21] Cyber criminals physically based in Ukraine have also begun to look for more comfortable conditions in which to operate, as Ukrainian law enforcement agencies have begun to collaborate with Western agencies.[22] Thus the number of cyber criminals in Ukraine may finally be declining.[23]

The conflict in eastern Ukraine has given rise to numerous high-level cyber attacks. As part of its military operations, Russia has used cyber warfare tactics against Ukrainian websites, some of which are physically hosted in Ukraine, while some are

11 Oleksandr V. Potii, Oleksandr V. Korneyko, and Yurii I. Gorbenko. 'Cybersecurity in Ukraine: Problems and Perspectives.' *Information and Security: An International Journal 32 (2015): 2.*
12 More detailed description will be provided later
13 Kostiantyn Kosrun, Skype Interview, July 6, 2015.
14 Glib Pakharenko, Interview, June 29, 2015.
15 ₴ – Hryvnia – Ukrainian unit of currency.
16 As mentioned by Guzii who works at the MVD department that deals with card (credit and debit) fraud operations.
17 Supra, note 14; supra, note 7.
18 The interviewee referred to the fact that it became quite hard for hackers to operate in Russia without being under constant government control.
19 Supra, note 7.
20 Glib Pakharenko, e-mail to the author, July 5, 2015.
21 *Ibid*.
22 *Ibid*.
23 *Ibid*.

not.[24] National Security Agency (NSA) Director Vice Admiral Michael Rogers stated that Russia conducted cyber operations to support its Crimea conquest.[25] Independent researchers also discovered a cyber espionage operation called Armageddon that was designed to provide a 'military advantage to Russian leadership by targeting Ukrainian government and law enforcement agencies',[26] and included DDoS attacks against Ukrainian and NATO media outlets, and targeted attacks against Ukrainian election commission websites.[27] In all, hackers hit Ukrainian government, business, online media, and e-commerce sites.[28] Finally, it should be noted in this context that Ukraine's information and telecommunication networks generally use Russian hardware and software, a situation that would significantly help Russia to spy on its southern neighbour.[29]

4 Ukraine's Cyber Security Agenda

While cyber crime has flourished in Ukraine, the same cannot be said for the development of Kyiv's cyber security policy, which is simply not currently a high priority. In Ukraine, only 41.8% of the population is now online, compared to 84.2% in the United States and 61.4% in Russia.[30] Furthermore, the majority of Ukrainian internet connectivity lies in the country's major cities and very few electronic devices are used for online financial transactions.

While cyber crime has flourished in Ukraine, the same cannot be said for the development of Kyiv's cyber security policy.

Currently, there is little cyber security legislation in Ukraine. The more prominent laws include 'On Information,' 'On State Secrets,' 'On Data Protection in Information and Telecommunication Systems,' 'On the National Security of Ukraine,' and 'On State Service for Special Communication and Information Protection of Ukraine.' In 2012, Parliament began to propose amendments to these laws. Today, there is an increasing focus on cyber crime awareness, and the government is in the process of creating a new ministry devoted to information technology (IT).

24 Sam Jones. 'Ukraine PM's Office Hit by Cyber Attack Linked to Russia.' *Financial Times*, August 7, 2014. http://www.ft.com/intl/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html.

25 Bill Gertz. 'Inside the Ring: Cybercom's Michael Rogers Confirms Russia Conducted Cyberattacks against Ukraine.' *Washington Times*, March 12, 2014. http://www.washingtontimes.com/news/2014/mar/12/inside-the-ring-cybercoms-michael-rogers-confirms-/?page=all.

26 'LookingGlass Cyber Threat Intelligence Group Links Russia to Cyber Espionage Campaign Targeting Ukrainian Government and Military Officials.' *Looking Glass*, April 29, 2015.

27 Tony Martin-Vegue. 'Are We Witnessing a Cyber War between Russia and Ukraine? Don't Blink – You Might Miss It.' CSO Online, April 24, 2015. http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html.

28 Primarily with DDoS attacks from supra, note 11.

29 For example, via Russia's Система Оперативно-Розыскных Мероприятий, or 'System for Operative Investigative Activities', a technical system run by the Russian security services to search and surveil telephone and Internet communications. Supra, note 11, page 2; Andrei Soldatov, Skype interview, July 15, 2015.

30 'Online Panel Ukraine and Online Data Collection Ukraine | DataDiggers Online Data Collection.' DataDiggers Online Data Collection. July 27, 2015. http://www.datadiggers.ro/?page_id=75217.

Victor Zhora, CEO and Co-Founder at Infosafe IT LLC, contends that a major problem with existing Ukrainian legislation is the lack of a clear definition for cyber crime. The only operational definition is in Article 361 of the Criminal Codex of Ukraine: 'Illegal interference with the operation of computers (PCs), automated systems, computer networks or telecommunications networks'.[31] However, it is not clear what 'illegal interference' actually means.

Recently, lawmakers have considered new legislation – the 'Cybersecurity Law of Ukraine' – which seeks to: update existing laws; create conditions for cooperation between the private and publics sectors; protect critical information infrastructure; develop a comprehensive legal framework; build a secure national security network; educate future specialists; fight cyber crime and cyber terrorism; strengthen the state's defence in cyberspace; prevent other states from interfering in Ukraine's internal affairs; neutralise attacks on Ukraine's information resources; and ensure Ukraine's full participation in European and regional cybersecurity organisations. [32] However, such a comprehensive agenda faces numerous acute challenges before it can be properly implemented.[33]

For example, 'the strategy of creating a secure national segment of cyberspace' lacks a working definition of critical national infrastructure (CNI), as well as a valid list of CNI. At this stage in Ukraine's economic development, there is little CNI with internet-based management, but that number is beginning to rise.[34] Another example is 'ensuring full participation of Ukraine in European and regional systems'. Although Ukrainian cyber security experts already share information and intelligence with Western colleagues, this collaboration is not nearly as effective as it could be, because the West does not yet 'respect [them] and do not share information with [them].'[35]

For the foreseeable future, Ukrainian CNI will rely on reasonably sound private sector approaches.

It is debatable, given the ongoing war in eastern Ukraine, how urgent this process is, especially given that all countries are currently struggling to protect CNI. Even if adopted, the draft Cybersecurity Law of Ukraine will take years to fully implement.[36] Therefore, for the foreseeable future, Ukrainian CNI such as telecoms,[37] banks,[38] and insurance companies[39] will rely on reasonably sound private sector approaches to their cyber security challenges.[40]

31 'Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'явку; supra, note 1.
32 Supra, note 11, figure 1-1.
33 Some of those challenges were mentioned earlier.
34 Ukraine's CNI objects are not controlled via the Internet, as mentioned in the skype interview with Vlad Styran on July 6, 2015 (Supra, note 7).
35 Supra, note 14.
36 Its implementation has three stages: 1) 2014-2016; 2) 2016-2017; and 3) 2017 – the following years.
37 Telecom operators are mostly protected as a huge portion of the population uses these services. They do no necessarily suffer from cyber attacks but they suffer from their clients' abuse of the system. From supra, note 7.
38 Banks are in second place in terms of protection and in first place in terms of damage.. It is quite a new trend in Ukraine as banks mostly operate using their clients' money. Last year, we witnessed the first cyber attacks on Ukrainian banks. From supra, note 7.
39 Insurance companies take the third place on the level of protection. They are active in protecting their companies from cyber attacks not because they are subjects to those attacks, but mostly because they are part of some international group, which requires them to follow the EU or U.S. requirements or because they need to create their image. Supra, note 7.
40 *Ibid*.

Figure 1-1 – Organisation of the cyber security system of Ukraine

5 Cybersecurity Organisations

Figure 1-1 depicts Ukraine's governmental organisations that deal with cyber crime: the Security Service of Ukraine (SBU); the State Service of Special Communication and Information Protection of Ukraine (SSSCIP); the Ministry of International Affairs of Ukraine (MVS) with its Department on Combating Cybercrimes; the Ministry of Defence of Ukraine (MO) with its Electronic Warfare Troops; the Defence Intelligence Service; and the Foreign Intelligence Service.[41] These agencies, of course, have different domains and priorities, and they rarely collaborate on common problems.[42] For example, MVD cyber units have a difficult time working with the SBU, which does not focus on external affairs, a crucial element in locating international hackers.[43] Glib Pakharenko, the ISACA Kyiv Chapter membership director, said: 'When NATO meets with various cyber forces in Ukraine, they only observe how these forces fight with each other and blame each other for failures'.[44]

SSSCIP is the only organisation that works exclusively on cyber security issues. Its main activities include: 'interaction with the administration domain UA.; protection of state information resources; interaction with state authorities; international cooperation in the protection of information resources; unified antivirus protection system; and determining the level of protection of information and telecommunication authorities' systems.'[45] SSSCIP has numerous internal offices, including the Centre for Antivirus Information Protection (CAIP),[46] the Assessment of Protection of State Information Resources, the Cybernetic Protection System, and the Registry

41 Supra, note 11.
42 Supra, note 7.
43 *Ibid*.
44 Supra, note 7.
45 Supra, note 39.
46 Supra, note 11.

of Information and Telecommunication Authorities' Systems. Its Computer Emergency Response Team of Ukraine (CERT-UA) handles international cooperation.

Each agency faces its own unique challenges and suffers from its own, unique criticism. For example, one interviewee said of CERT-UA: '[its specialists] just visit Europe and tell [the Europeans] how amazing they are. They [only] do PR and make contacts in Ukraine and abroad.'[47] Others, however, disagreed, arguing that in 2013 CERT-UA processed 232 incident reports from foreign CERTs[48] and was 'quite effective' despite 'significantly limited powers', a lack of qualified specialists, insufficient resources, and a low level of outside trust.[49] Two interviewees, Kostiantyn Korsun of Berezha Security and Glib Pakharenko of ISACA Kyiv, added that CERT-UA's bigger problem is the country's almost exclusive current focus on fighting Russian aggression in eastern Ukraine.[50]

CERT-UA's bigger problem is the country's almost exclusive focus on fighting Russian aggression in eastern Ukraine.

At the MVD, Vasyl Guzii, a specialist in *kartkove shakhraistvo* (credit card fraud operations), asserted that no '*sdelka iz pravosudiiem*' ('deal with law enforcement agencies' in Russian) exists in Ukraine.[51] However, Styran was not so sure, suggesting that '*verbyvannia*' ('recruitment') was common.[52] In effect, this means that instead of arresting hackers, law enforcement agencies simply offer *krysha* (protection)[53] in exchange for future favours.[54] The overall level of corruption in Ukraine is high, even at the SBU.[55]

Despite everything, there is progress to report. Beyond the new draft law on cyber security and the proposed new IT ministry[56] Ukraine is setting up an Interagency Board[57] to counter strategic cyber threats (see Figure 1-2). This initiative will of course take time to blossom, and there are already doubts about technical talent, bureaucratic implementation, and overall SBU power in this new initiative.[58] So, for the time being, it is likely that the Ukrainian government will continue to rely on an approach favoured in the United Kingdom: *pereklastu* or delegating many cyber crime-related tasks, including client protection, to the private sector.[59]

47 Supra, note 7.
48 Supra note, 11.
49 "незважаючи на суттєве обмеження повноважень в сфері розслідування комп'ютерних злочинів (це не належить до їхньої компетенції), відсутність достатньої кількості кваліфікованих фахівців, недостатні матеріальну базу та рівень фінансового забезпечення, низький рівень довіри з боку як бізнес-структур, так навіть і органів державної влади." Supra, note 1.
50 However, Korsun pointed out that nearly all countries – especially in Eastern Europe – face the same challenges of low salaries and poor skillsets. He added that the SBU, in this regard, is not so different to CERT-UA. Supra, note 13.
51 Vlad Styran. 'Securit13 Podcast : Эпизод 30: Let the Magic Begin.' March 20, 2015. http://securit13.libsyn.com/-30-let-the-magic-begin.
52 Supra, note 7.
53 'Roofing' means that the law enforcement agencies do not pay attention to criminal's misbehavior in exchange for favors.
54 Supra, note 14.
55 *Ibid.*
56 Ol'ha Karpenko. 'В Украине создадут министерство IT.' *AIN*, June 18, 2015. http://ain.ua/2015/06/18/586897.
57 Supra, note 11.
58 Филипповский, Игорь. ЛІГАБізнесІнформ, June 25, 2015. http://biz.liga.net/all/it/stati/3046442-deputaty-doshli-do-interneta-est-zakonoproekt-o-kibeprostranstve.htm.
59 Supra, note 7.

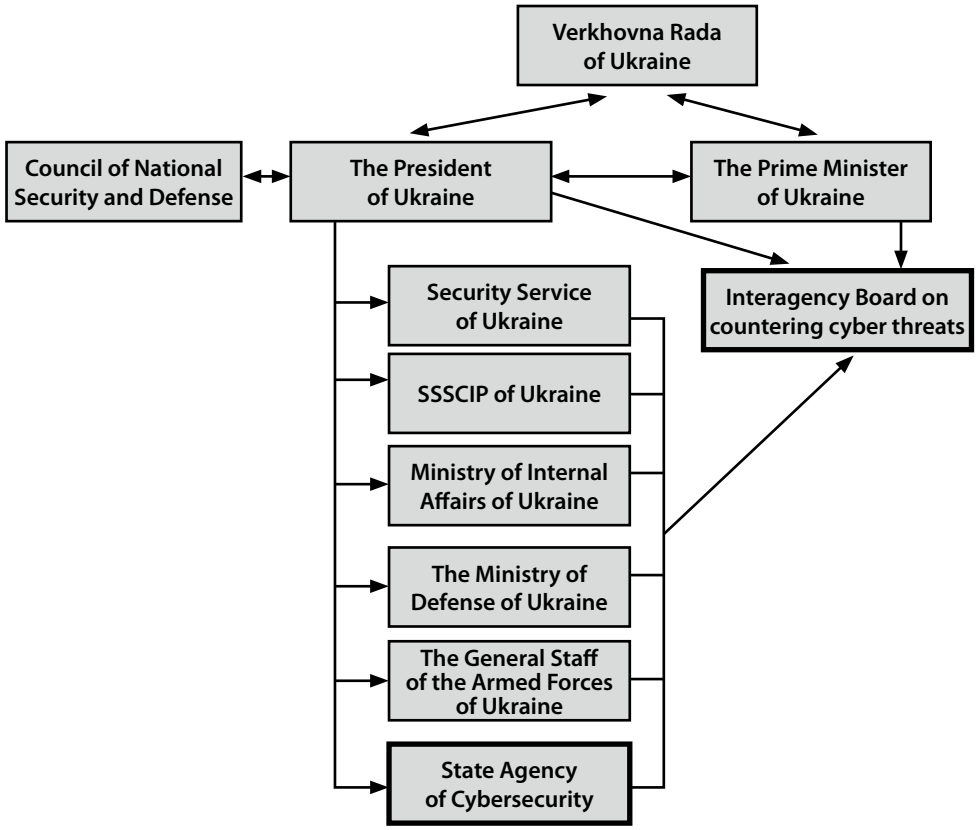

Figure 1-2 – Proposed organisation of Ukraine's system for cyber security

6 Recommendations

The following 'best practices' could significantly strengthen Ukraine's cyber security posture for the future.

6.1 National

- Metrics. Analysts believe that cyber crime is rife in Ukraine, but there are no accurate measurements or reliable studies that have documented this problem. Some Western[60] and Ukrainian companies[61] are now addressing this issue, but without better data and analysis, it is hard to separate fact from fiction.
- Prevention. Until Ukraine invests more in proactive cyber defence, it will remain in a reactive mode *vis-à-vis* cyber criminals, a serious problem in the age of light-speed communications.

60 Such as RAND.
61 Supra, note 14.

- Corruption. Ukraine must address bribes, protection,[62] and the unethical recruitment of hackers. In one infamous case, a fraudulent cyber crime 'call centre', which in fact was used to steal credit card information, actually operated from a Ukrainian prison.[63]
- Culture. Ukraine must promote cyber crime awareness and enforce existing law. Ukrainian citizens must recognise that stealing money from the West is against the law, and they must be willing to report such crimes to law enforcement.[64]
- Education. Kyiv must invest in the academic side of cyber security, to include software engineering, critical infrastructure protection, and more.[65] Some steps have already been taken, including the creation of *kiberpolitseiski* (cyber police) departments at the Kyiv and Kharkiv MVD Institutes;[66] further, the MVD has collaborated with various departments of the Kyiv Polytechnic Institute (KPI). The Science Park of the KPI promotes science-intensive products on domestic and foreign markets that provide better cybersecurity solutions. [67,68]
- Civil Society. The Ukrainian Government requires pressure from below to assist in the implementation of so many needed changes. Even from abroad, the Ukrainian diaspora can help.
- Oversight. Ukrainian lawmakers often receive foreign assistance to help the country adopt and implement reform, but currently there is no effective oversight body helping to manage this process.[69]
- Public sector labour force. The Ukrainian government must find a way to hire qualified cyber security professionals and retain them with quality training and attractive salaries. It must be said that this challenge is not unique to Ukraine.[70]

6.2 Regional and International

- Collaboration. Ukrainian cyber security institutions must develop a higher level of trust with their international counterparts, especially in the West. This begins with practical cooperation on current high-interest criminal cases, to include resource and information sharing. In the past, such collaboration has not always been effective, and sometimes never occurred at all.[71] Points of departure include Mutual Legal Assis-

62 *Ibid*.
63 Supra, note 7.
64 These two measures will be discussed later.
65 So far, eighteen universities carry out training specialists in information security on bachelor's and master's levels in Ukraine. From: Standards of higher education 1701 'Information Security,' accessed on July 21, 2015, http://iszzi.kpi.ua/index.php/ua/biblioteka/normativno-pravova-baza/nmk-informatsijna-bezpeka.html .
66 Supra, note 50.
67 *Ibid*.
68 'Science Park 'Kyivska Polytechnika." Accessed September 1, 2015.
69 Supra, note 7.
70 Supra, note 14.
71 *Ibid*.

tance Treaties (MLAT) and the European Convention on Cybercrime which Ukraine ratified in 2005.

- Western Assistance. Most of the digital equipment in Ukraine was manufactured in Russia, so there is an urgent need for EU and NATO nations to assist Ukraine in replacing it. Some concrete steps have already been taken: NATO has allocated funds for Ukraine's 'cyber defences, command and control structures, and logistics capabilities';[72] Microsoft announced a partnership with the Ukrainian Government on cyber security;[73] U.S. Senators Mark Kirk and Mark Warner announced a 'bipartisan amendment creating a law enforcement partnership between the United States and Ukraine to combat cybercrime and improve cybersecurity';[74] and Romania launched an initiative to support the Ukraine Cyber Defence Trust Fund.[75]
- Cyber security strategy. Ukraine must harmonise its cyber security policies and legislation with those of the most technologically advanced members of the international community. The European Network and Information Security Agency (ENISA) has a strong record of providing guidance in cyber security policy development and best practices; Ukraine should take full advantage of this resource.

7 Conclusion

Ukraine, with its talented hackers and minimal cyber security regulations, is a perfect case study to examine the many challenges that Eastern European countries face as they seek to improve their cyber security posture. Ukraine has more than enough STEM expertise, but it must be refocused and repurposed toward a more transparent and accountable legal and cultural online environment. The development of Ukrainian civil society can accomplish all of these objectives, but the international community – including the Ukrainian diaspora – can help Kyiv to realise them much more quickly. Unfortunately, however, Ukraine's current political, economic, and military crises are likely to prevent it from climbing down the world's cyber crime ladder in the near term.

> *Ukraine has more than enough STEM expertise, but it must be refocused and repurposed.*

72 Andrew Rettman. 'Mr. Putin Isn't Done in East Ukraine.' *EUObserver*, June 26, 2015. https://euobserver.com/defence/129317.

73 'Ukrainian Government Partners with Microsoft on Cyber Security.' *Ukrainian Digital News*, April 7, 2015. http://uadn.net/2015/04/07/ukrainian-government-partners-with-microsoft-on-cyber-security/.

74 'Kirk, Warner to Introduce Cybersecurity Amendment to Ukrainian Aid Bill on Monday.' *Kirk Senate*. March 23, 2014. http://www.kirk.senate.gov/?p=press_release&id=1033.

75 'Romania Turns Hacking Crisis into Advantage, Helping Ukraine Fight Russian Cyber Espionage.' *Azerbaijan State News Agency*, May 18, 2015. http://azertag.az/en/xeber/Romania_turns_hacking_crisis_into_advantage_helping_Ukraine_fight_Russian_cyber_espionage-855844.