УДК 330:30 ; 004.056
Peter Debbins
JEL Classification F50, K24 J28

SECURING UKRAINE THROUGH CYBER FINANCIAL CRIMES MITIGATION

This article posits that the first approach to develop a culture of Cyber and Information Technology (IT) for Ukraine's overall economic and strategic security should begin with the development and implementation of Cyber Financial Crimes Mitigation training for the senior managers and executives of Ukrainian enterprises. Because Cyber Financial Crimes have the most direct impact to that group and they have the means to address it, they are the group who can impart a culture of IT and Cyber Security to Ukrainian society and leadership.
Keywords: *Cyber and Information Technology; Cyber Financial Crimes; Cyber Security; economic and strategic security.*

DOI 10.37659/2663-5070-2019-3-25-30

Framing the Question

As the world completes "The Industrial Revolution 4.0" in which nearly every aspect of human existence has been digitized, the field of Cyber Security is now so broad that attempting to form a unified approached to all threats is rendered impossible. Instead, when looking at the problem, or rather the question of how does Ukraine improve her Cyber Security to protect her economic and strategic well-being, we should look at one specific area that will have great impact, which is the mitigation of Cyber Financial Crimes. We use the term "Mitigation" and not "Defeat" because in the area of law enforcement, crimes can only be battled and their impacts reduced, but never defeated.

At the time of this article's writing (April 14, 2020), the attention of the whole world is focused on mitigating the impact of the COVID-19 pandemic. However, the plague of Cyber Financial Crimes continues unabated. During this time of self-quarantine cyber-security stakeholders can still look at how to mitigate Cyber Financial Crimes which are adversely impacting Ukraine's security and development. So, when the COVID-19 pestilence abates, Ukrainian cyber-security stakeholders can begin to execute various solutions.

- What are Cyber Financial Crimes?
- How are they unique from the other Cyber Security disciplines?
- Do all cyber-attacks inflict a financial cost?

This article will define Cyber Financial Crimes as the use of cyber and information technology (IT) means to manipulate or alter an enterprise's **accounting** and **auditing** processes to inflict financial loss on the enterprise and/or its customers.

This clear distinction is critical, so cyber-security stakeholders focus on how to implement cyber-security disciplines on the areas of accounting and auditing. This is important because current approaches to Cyber and IT Security generally separate the disciplines of Cyber Security from Accounting and Auditing.

Current Approach

According to most estimates, the world is spending close to $250 billion per year on Cyber Security. However, that number doesn't encompass all the resources and time spent on Cyber Security, such as the increased cost of hardware and software to ensure security, and then the training and practices for workforces. Taking those factors into account raises the estimated cost of cyber security to close to $1 trillion (USD), roughly 1% of the world's annual income [1].

With all this spending what are the results? According to John Strand, who recently publish a book advocating Offensive Countermeasures (aka "Hack Back"), he states that

> "*When we objectively look at information security today, it is easy to see that many of the various techniques we use for defense fall somewhere between not working and barely working at all*." [1]

As a result, organizations and enterprises continue to suffer enormous financial losses. The cost in financial terms (not counting reputational, morale, degraded performance, and future impacts) for the world economy is close to an additional 1% of its annual income [2].

The United States is by far most advance in cyber security, due to its long-standing IT security culture, driven and fostered by its robust IT commercial sector which started in 1844 with the first commercial electric telegraph. So, it should be a model for the world. However, surveys of the thousands of professional training programs and academic institutions will show little in fusing the disciplines of Cyber Security, Accounting, and Auditing [3]. Instead of fusion in cyber-crime investigations, there are clear distinctions between Anti-Money Laundering (AML), cyber-attacks, and accounting. When we look at Europe, we likewise see a lack of fusion among the disciplines. And, in comparison to the US, Europe can be regarded as five years behind whatever the US is doing in the field of cybersecurity [4].

Ukraine's Cyber Security Landscape

Ukraine can be described as a neophyte when it comes to incorporating cyber security into her culture and as a Core Business Function. There are several reasons for this situation:

- First, Ukraine still does not have IT culture that permeates most aspects of society (something which the US had since the early 1990s).
- Second, given its weaker economic standing, less resources are available to the digitization of the society and economic activities.
- And third, there is a lack of knowledge and understanding of the how Cyber Financial Crimes are occurring.

Yet, the reporting about Cyber Security in Ukraine looks at two different aspects: The first is Ukraine's cyber vulnerability in geopolitical competition, and the second is Ukraine as a safe haven for cyber criminals.

When we look at those two aspects, we should see them as the **result** of a weak cyber security culture, and less as a **cause**. The 2015 Attack of the Electrical Grid was result of poor organizational practices which allowed a Microsoft Excel document to be the payload of the malware. The relative ease of cyber criminals to operate is partly a lack of secure licit IT and Cyber Security employment for highly skilled professionals and partly a lack of societal understanding of what constitutes illicit behavior.

Addressing the issues facing Ukraine's cyber security may seem too daunting to resolve; however, there is an opportunity to conduct a **targeted** approach in one area, Cyber Financial Crimes. This can have a multiplier effect on Ukraine's IT security culture and overall national security and economic well-being. It has the added feature that Ukraine could emerge as a leader in the undeveloped discipline of global Cyber Security.

Ukraine's Potential

Looking at the impact of Cyber Financial Crimes, Ukraine has a unique potential, primarily because it stands out as being considerably behind other nations in using advanced techniques in combating fraud [5]. In their ***Global Economic Crime and Fraud Survey 2018: Ukrainian findings: Pulling fraud out of the shadows***, the international auditing and accounting consulting firm, PwC (PricewaterhouseCooper) details the large potential for improvement for Ukraine. When looking at their survey result (see Figure 1), not only would Ukraine gain the most by bringing in best practices, but Ukraine would also develop unique approaches and expertise as she closes the gap. Ukraine would be learning and developing cyber tools to mitigate financial crimes.

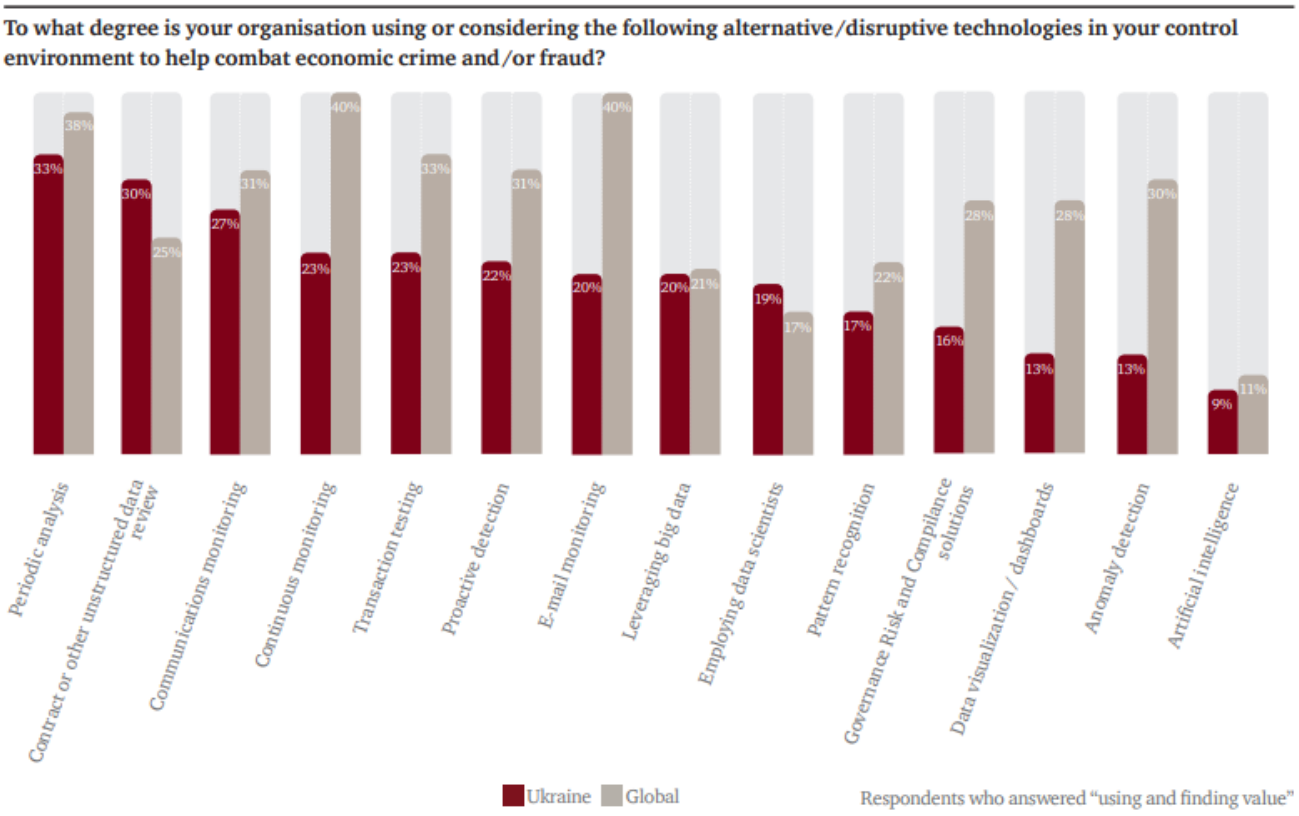

Fig. 1. *PwC 2018 Survey Results*

However, let us look at the reality of Ukraine's deficiencies. Her enterprises are victims of financial crimes that could have been mitigated by standard and advance cyber tools and means. And it is only worsening, in the 2018 year report, 48% of respondents in Ukraine said their organizations had suffered from fraud in the last two years, up from 43% in 2016 [6]. These tools could mitigate bribery and corruption which impacted 73% of Ukrainian organizations per the report. Effective Cyber Financial Crimes training and practicing can mitigate the other top four reported economic crimes:

- asset misappropriation,
- procurement fraud,
- human resources (HR) fraud, and
- cybercrime (monetary and intellectual theft, disruptions, and data loss).

And even with the losses and ubiquitous coverage of cyber-crimes, only 1 in 3 organizations in Ukraine have a cyber security program [7]. In contract, nearly every US enterprise has a cyber security program.

These financial crimes have an enormous cost for an emerging economy. An American firm can weather a loss of $100,000 (the average annual cost of an employee), but that amount would be devastating for a Ukrainian firm. Of the Ukrainian companies surveyed by PwC in 2018, 12% had losses between 1 and 50 million dollars US (see Figure 2). And not just monetary losses, but these firms faced additional costs in reputation, brand strength, business relations, and relations with regulators. Most disheartening is the damage on employee morale and productivity.

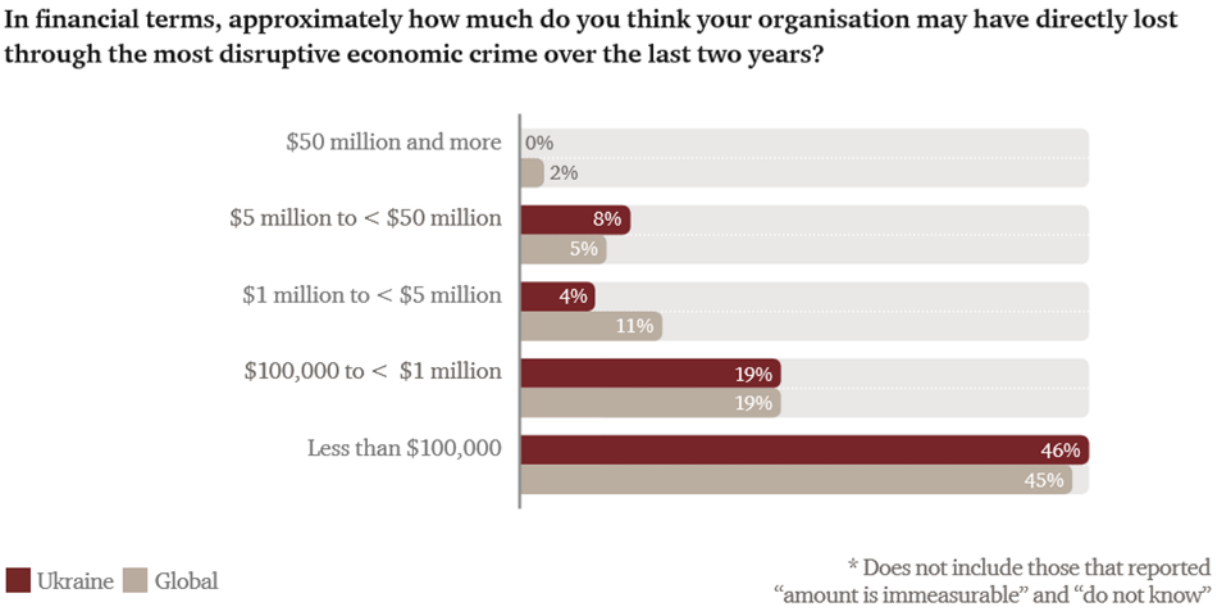

Fig. 2. *PwC 2018 Survey Results*

Mitigating Cyber Financial Crimes would help address Ukrainian enterprises' biggest weakness to fraud: the third parties with whom the enterprises have regular and profitable relationships, the agents, vendors, and customers.

A certain degree of mutual trust is expected; however, this trust cannot be verified nor theft detected because a comprehensive approach to accounting and auditing, to utilizing cyber tools are not known or employed. When used these approaches can protect an enterprise. Per the survey, 49% of Ukrainian enterprises reported that technology tools enable them to carry out real-time monitoring and 51% stated it provided them with actionable insights. We must ask,

What is causing 50% of the other firms not to use them or not achieve any benefits?

What is to be done?

A preponderance of articles written on the topic of Cyber Financial Crimes in Ukraine (or elsewhere for that matter) will often recommend that the government take the lead on providing cyber security. While at the same time, these articles bemoan the fact that bifurcated government agencies generally do not cooperate. Even agencies in open, accountable governments in Europe and the United States will not share information yet will swiftly pass blame to other agencies for failures. We must accept this as the nature of any government organization, and we must look to develop a new way to transform the cyber security environment. If we look at past societal changes, they generally start with key influencers, a small percentage of the population who are the senior managerial class, who drive change and can deliver transformation of a society's knowledge, skills, and attitudes (KSAs). Transforming Ukraine into an IT security-conscious culture (similar to the US) and conducive to discouraging cybercrime will require a targeted and incremental approach.

If we look at the case of the forces that caused the Soviet Union to collapse, the biggest drivers of Perestroika, Glasnost, and the eventual dissolution of the USSR, were not the impoverished classes (the overwhelming majority) nor the elites of the Politburo and upper echelons of the Party. Rather, the drivers were the middle and upper managerial classes who had the most contact with their counterparts in the liberal, capitalist societies. They insisted on the change, having more to gain by change than by maintaining the status-quo [8].

A "top-down" approach is not effective, since top management is rotated out via elections, personnel turnover, bureaucratic obscuration, and the occasional revolution. A "bottom-up" approach for extensive topic such as cyber security is not likely to succeed. Transformation of KSAs one person

at time is simply too slow in the rapidly changing cyber-security environment. Often the general populace, as seen with social media campaigns, is often misled by false information and rumors, or ineffective feel-good fad and trends.

A "middle-out" approach is the most effective way to transform societal KSAs.

- First, the middle and upper managers are the people who have the positions and authorities to implement cyber-security practices.
- Second, they have the competence, knowledge, and experience to assess the value and weigh the costs.
- Third, they have influence on their workforce cadre, who are the majority of society, and on their superiors, the country's leaders, who create the laws and the frameworks to ensure cyber security.

Why address Cyber Financial Crimes as the first topic of many in cyber security?

Because Cyber Financial Crimes have the most direct impact to Ukraine's senior managers and executives. They have the means to address it. They are the group who can impart a culture of IT and Cyber Security to Ukrainian society and leaders. Cyber security is *terra incognito* for many because it is presently a realm exclusive to IT security specialists -- the personnel who have the technical skills to protect, by technical means, an organization from cyber-attacks.

However, as illustrated by the PwC 2018 Report on Ukraine, there is little translation of cyber tools and cyber security from a technical realm to one that managers and executives can apply to their financial realm. A Cyber Financial Crimes discipline would present senior managers and executives with the means to apply effective cyber tools and good cyber practices to ensure accounting (cash flow) and auditing (transparency).

Delivery

In our current world, what institutions can change the KSAs of the managerial class?

There are three key institutional change mechanisms:

- Higher Education (Universities and Colleges),
- Professional Training Institutes (such a SANS.org), and
- Professional Associations (Chambers of Commerce, PMI, ISSA - Information Systems Security Association).

Often professional societies operate training institutes [9]. As of 2015, there were 15 Ukrainian universities providing training in cyber security [10] and as of 2020 there is likely more working in some capacity. However, similar to the rest of the world, the current professional cyber-security training community emphasizes technical means. If that separation of disciplines continues, the managers and executives of Ukrainian enterprises will find it hard to establish a cyber- security culture.

Implement

Given the lack of fusion among the disciplines of Cyber Security, Accounting, and Auditing and an absence of training enterprises that could deliver it to Ukraine's senior managers and executives, there is a unique opportunity to develop global center of excellence (COE) in Cyber Financial Crimes mitigation. This COE would bring in the key Ukrainian stakeholders: academia, government agencies and enterprises, commercial business enterprises, profession training organizations, and professional associations. This COE would also involve cyber-security stakeholders outside Ukraine as well.

The vision of such of COE should treat Cyber Financial Crimes as a study, and not as a science, taking the quote from Nassim Taleb's 2007 bestseller, ***The Black Swan: The Impact of the Highly Improbable:***

> *Things that move (are dynamic) don't seem to have experts. Simply, things that move, and therefore require knowledge, do not usually have experts, while things that don't move seem to have some experts.*

This approach would engage senior managers and executives who lack either the confidence or expertise to engage the problems of Cyber Financial Crimes. The COE has the goal of providing the

knowledge, methods, and protocols to its stakeholders so they **know** the questions to ask, **understand** the answers, and effectively **utilize** cyberspace to promote and protect their enterprises.

If Ukraine emerges as a leader in the study and mitigation of Cyber Financial Crimes, she has the unique opportunity to develop a global niche for its IT industry and professionals, enhance her economic growth, and strengthen her strategic security.

References

1. Forbes: Apr 23, 2018, Remington Tonar and Ellis Talton:
A Lack Of Cybersecurity Funding And Expertise Threatens U.S. Infrastructure. Retrieved from https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#1846e7ac49e0 on April 13, 2020
2. Merchant Risk Council (MRC) Blog: Issue 27: *Financial Impacts of Cybercrime*. Retrieved from https://merchantriskcouncil.org/news-and-press/mrc-blog/2018/financial-impacts-of-cybercrime on April 13, 2020
3. Only one US academic institutions, The Economic Crime and Cybersecurity Institute of Utica College (ECCI), has a program fusing those three disciplines. None were found in Europe. Retrieved from google query terms [*"cyber financial crimes"+degree+programs*], viewing 20 page results on April 13, 2020.
4. According to a November 14, 2019 interview with Alain Establier, Editor in Chief of SDBR NEWSS Security Defense Business Review http://www.sdbrnews.com as well analysis by New America's Cyber Security Initiative. Retrieved from https://soundcloud.com/newamerica/the-state-of-cybersecurity-in-asia?in=newamerica/sets/the-cybersecurity-podcast on April 13, 2020.
5. PriceWaterhouseCooper (PwC) *Global Economic Crime and Fraud Survey 2018: Ukrainian findings Pulling fraud out of the shadows.* Retrieved from
https://www.pwc.com/ua/en/survey/2018/pwc-gecs-2018-eng.pdf April 13, 2020
6. ibid
7. ibid
8. *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It, Chapter 4: Avalanche Country* Joshua Cooper Ramo ©2009
9. Cyber Crime Magazine: *Cybersecurity Industry Associations.* Retrieved from https://cybersecurityventures.com/cybersecurity-associations/ April 14, 2020
10. NATO Cooperative Cyber Defence Centre of Excellence: Cyber War in Perspective:
Russian Aggression against Ukraine, Chapter 13: *Ukraine: A Cyber Safe Haven?* Nadiya Kostyuk NATO CCD COE Publications, Tallinn 2015. Retrieved from
https://ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf April 14, 2020

Петер Деббінс

Захист України шляхом зменшення кібер-фінансових злочинів

У статті стверджується, що перший підхід до розвитку культури кібернетичних та інформаційних технологій (ІТ) для загальної економічної та стратегічної безпеки України повинен розпочатися з розробки та впровадження навчання з питань зменшення кібер-фінансових злочинів для вищих керівників та керівників українських підприємств. Оскільки кібер-фінансові злочини мають безпосередній вплив на цю групу, вони повинні мати засоби для її подолання і таке навчання зможе надавати необхідну культуру використання ІТ та кібербезпеки українському суспільству та її лідерам.

Ключові слова: *кібер та інформаційні технології; Кіберфінансові злочини; Кібербезпека; економічна та стратегічна безпека.*