

CyBOK

The Cyber Security Body Of Knowledge



CyBOK Wiki: Feasibility study

CyBOK Funded Project

contact@cybok.org
www.cybok.org

Hi!

Lőrinc Thurnay *(Lawrence)*
research associate
Center for e-Governance

Research interests:

- Open data applications
- Open legal data
- ML/NLP
- Cyber-security

loerinc.thurnay@donau-uni.ac.at

University for
Continuing
Education Krems



Motivation for CyBOK Wiki

CyBOK is >1000 pages, PDF only

Linear, but I need to browse and explore

Could it be released as a Wiki platform?

- | | |
|-------------------|--|
| User eXperience → | search, smart recommendations, multi-tab, copy/paste |
| Accessibility → | responsive to screen size, screen readers |
| Discoverability → | SEO, links to individual (sub)sections |

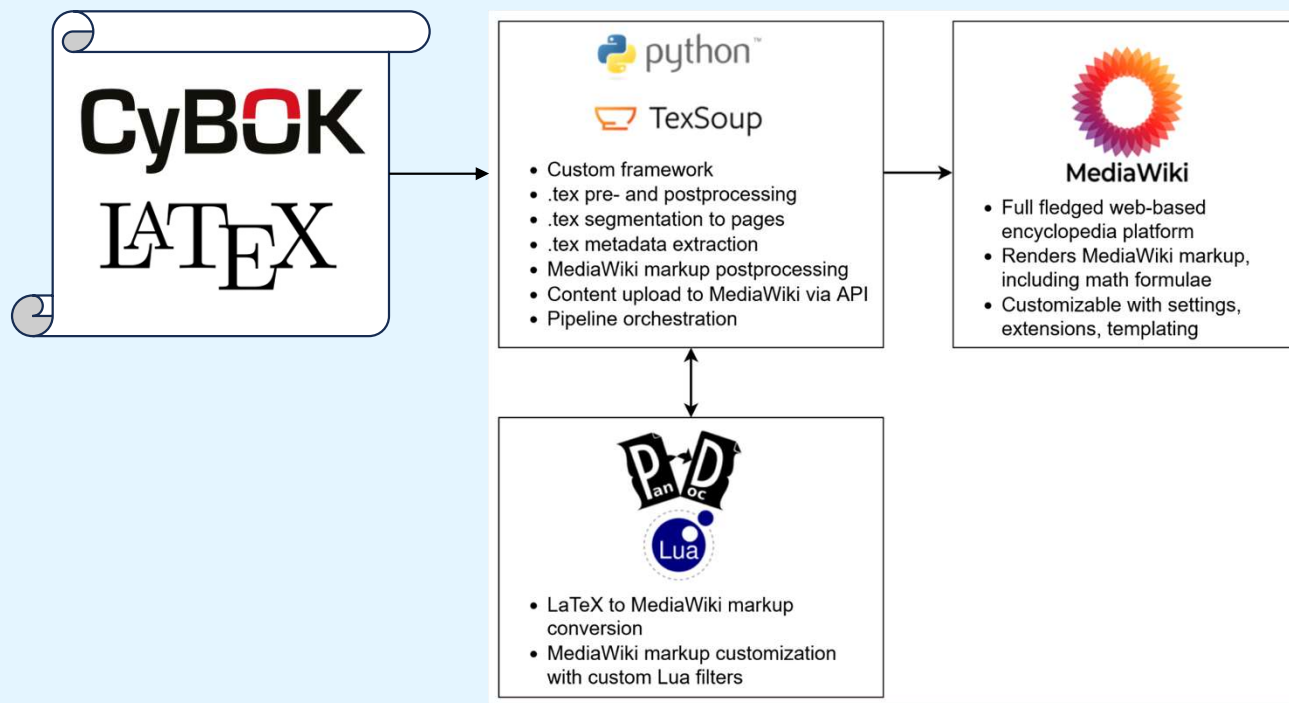
Feasibility study

RQ: Is CyBOK Wiki technically feasible – and how?

Proof-of-concept software

Based on 3 KAs

Software proof-of-concept



- **Segmentation**
(sub)chapters to Wiki articles
- **Conversion**
LaTeX code to Wiki markup
Custom preprocessors
and Pandoc
- **Publishing**
to MediaWiki instance

CyBOK Wiki Prototype

3 KAs into 118 Wiki pages
Not online

The screenshot shows a web browser window displaying the CyBOK Wiki page titled "A Characterisation of Adversaries". The browser's address bar shows the URL "127.0.0.1:8079/index.php/A_Characterisation_of_Adversaries". The page features a search bar, navigation links for "Create account" and "Log in", and a table of contents on the left. The main content area includes a "Parent chapter" link to "[Adversarial Behaviours]", a list of references, and a detailed paragraph discussing the motivation and characteristics of adversaries. A section titled "Cyber-enabled and cyber-dependent crimes" follows, with a list of five points explaining why the Internet facilitates such activities.

A Characterisation of Adversaries - X +

127.0.0.1:8079/index.php/A_Characterisation_of_Adversaries

CyBOK Wiki

Search CyBOK Wiki

Search

Create account Log in

A Characterisation of Adversaries

Page Discussion

Read Edit View history Tools

Contents [hide]

Beginning

- Cyber-enabled and cyber-dependent crimes
- Interpersonal offenders
- Cyber-enabled organized criminals
- Cyber-dependent organized criminals
- Hacktivists
- State actors

Parent chapter: [Adversarial Behaviours]

[1][2][3], [4][5], [6], [7][8][9], [10]

In this section, we present a characterisation of adversaries who perform malicious actions. This characterisation is based on their motivation (e.g., financial, political etc.). Although alternative characterisations and taxonomies exist (e.g., from the field of psychology[11]), we feel that the one presented here works best to illustrate known attackers' capabilities and the tools that are needed to set up a successful malicious operation, such as a financial malware enterprise. This characterisation also follows the evolution that cybercrime has followed in recent decades, from an ad-hoc operation carried out by a single offender to a commoditised ecosystem where various specialised actors operate together in an organised fashion[12], [13]. The characterisation presented in this section is driven by case studies and prominent examples covered in the research literature, and as such is not meant to be complete. For example, we do not focus on accidental offenders (e.g., inadvertent insider threats), or on criminal operations for which rigorous academic literature is lacking (e.g., attacks on financial institutions or supply chain attacks). However, we believe that the set of crimes and malicious activities presented is comprehensive enough to draw a representative picture of the adversarial behaviours that are occurring in the wild at the time of writing. We begin by defining two types of cyber offences as they have been defined in the literature, cyber-enabled and cyber-dependent crimes, and we continue by presenting different types of malicious activities that have been covered by researchers.

Cyber-enabled and cyber-dependent crimes [edit]

One of the main effects that the Internet has had on malicious activity has been to increase the reach of existing crimes, in terms of the ease of reaching victims, effectively removing the need for physical proximity between the victim and the offender. In the literature, these crimes are often referred to as *cyber-enabled*[1].

According to Clough[14], criminals have five main incentives to move their operations online:

1. Using the Internet, it is easier to find and contact victims. Email lists are sold on underground markets[15], while online social networks have search functionalities embedded in them, allowing criminals to easily identify potential victims[16], [17].
2. By using the Internet, criminal operations can be run more cheaply. Sending emails is free, while scammers previously had to pay postage to reach their victims. This also allows criminals to increase the scale of their operations to sizes that were previously unthinkable.
3. Compared to their physical counterparts, the Internet allows crimes to be performed faster. For example, emails can reach victims in a matter of seconds, without having to wait for physical letters to be delivered.
4. Using the Internet, it is easier to operate across international boundaries, reaching victims located in other countries. In this setting, often the only limitation is language, with criminals only targeting victims who speak a language that they are familiar with (e.g., people in English-speaking countries)[18].
5. By operating over the Internet, it is more difficult for criminals to get caught. This is mainly due to the transnational nature of cybercrime, and the fact that the problem of harmonising the appropriate laws of different countries is far from being solved[19]. In addition, research shows that

According to Clough [14], criminals have five main incentives to move their operations online:

1. Using the Internet, it is easier to find and contact victims. Email lists are sold on underground markets [15], while online social networks have search functionalities embedded in them, allowing criminals to easily identify potential victims [16, 17].
2. By using the Internet, criminal operations can be run more cheaply. Sending emails is free, while scammers previously had to pay postage to reach their victims. This also allows criminals to increase the scale of their operations to sizes that were previously unthinkable.
3. Compared to their physical counterparts, the Internet allows crimes to be performed faster. For example, emails can reach victims in a matter of seconds, without having to wait for physical letters to be delivered.
4. Using the Internet, it is easier to operate across international boundaries, reaching victims located in other countries. In this setting, often the only limitation is language, with criminals only targeting victims who speak a language that they are familiar with (e.g., people in English-speaking countries) [18].
5. By operating over the Internet, it is more difficult for criminals to get caught. This is mainly due to the transnational nature of cybercrime, and the fact that the problem of harmonising the appropriate laws of different countries is far from being solved [19]. In addition, research shows that online crime is often under reported, both because victims do not know whom to report it to (given that the offender might be located in another country), as well as the fact that they believe that they are unlikely to get their money back [20].

Cyber-dependent crimes, on the other hand, are crimes that can only be committed with the use of computers or technology devices [1]. Although the final goal of this type of crime often has parallels in the physical world (e.g., extortion, identity theft, financial fraud), the Internet and technology generally enable criminals to give a new shape to these crimes, making them large-scale organised endeavours able to reach hundreds of thousands, if not millions, of victims.

In the rest of this section we analyse a number of cyber-enabled and cyber-dependent criminal schemes in detail.

CyBOK PDF

Interpersonal offenders

The first category that we are going to analyse is that of *interpersonal crimes*. These crimes include targeted violence and harassment, directed at either close connections (e.g., family members) or strangers. While these crimes have always existed, the Internet has made the reach of harassers and criminals much longer, effectively removing the need for physical contact for the offence to be committed. As such, these crimes fall into the cyber-enabled category. In the rest of this section, we provide an overview of these adversarial behaviours.

Cyberbullying. Willard [2] defines cyberbullying as 'sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies'.

basic formatting citations

According to Clough[14], criminals have five main incentives to move their operations online:

1. Using the Internet, it is easier to find and contact victims. Email lists are sold on underground markets[15], while online social networks have search functionalities embedded in them, allowing criminals to easily identify potential victims[16], [17].
2. By using the Internet, criminal operations can be run more cheaply. Sending emails is free, while scammers previously had to pay postage to reach their victims. This also allows criminals to increase the scale of their operations to sizes that were previously unthinkable.
3. Compared to their physical counterparts, the Internet allows crimes to be performed faster. For example, emails can reach victims in a matter of seconds, without having to wait for physical letters to be delivered.
4. Using the Internet, it is easier to operate across international boundaries, reaching victims located in other countries. In this setting, often the only limitation is language, with criminals only targeting victims who speak a language that they are familiar with (e.g., people in English-speaking countries)[18].
5. By operating over the Internet, it is more difficult for criminals to get caught. This is mainly due to the transnational nature of cybercrime, and the fact that the problem of harmonising the appropriate laws of different countries is far from being solved[19]. In addition, research shows that online crime is often under reported, both because victims do not know whom to report it to (given that the offender might be located in another country), as well as the fact that they believe that they are unlikely to get their money back[20].

Cyber-dependent crimes, on the other hand, are crimes that can only be committed with the use of computers or technology devices[1]. Although the final goal of this type of crime often has parallels in the physical world (e.g., extortion, identity theft, financial fraud), the Internet and technology generally enable criminals to give a new shape to these crimes, making them large-scale organised endeavours able to reach hundreds of thousands, if not millions, of victims.

In the rest of this section we analyse a number of cyber-enabled and cyber-dependent criminal schemes in detail.

Interpersonal offenders [edit]

The first category that we are going to analyse is that of *interpersonal crimes*. These crimes include targeted violence and harassment, directed at either close connections (e.g., family members) or strangers. While these crimes have always existed, the Internet has made the reach of harassers and criminals much longer, effectively removing the need for physical contact for the offence to be committed. As such, these crimes fall into the cyber-enabled category. In the rest of this section, we provide an overview of these adversarial behaviours.

Cyberbullying. Willard[2] defines cyberbullying as 'sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies'. While not always illegal^[1], cyberbullying often occupies a grey area between what is considered a harmful act and

CyBOK Wiki

Bibliographies

[1] M. McGuire and S. Dowling, "Cyber crime: A review of the evidence," *Summary of Key Findings and Implications. Home Office Research Report*, vol. 75, 2013.

[2] N. E. Willard, *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research Press, 2007.

[3] H. Glickman, "The Nigerian '419' advance fee scams: Prank or peril?" *Canadian Journal of African Studies/La Revue Canadienne Des Études Africaines*, vol. 39, no. 3, pp. 460–489, 2005.

[4] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *International Conference on World Wide Web (WWW)*, ACM, 2013, pp. 213–224.

[5] C. Kanich *et al.*, "Spamalytics: An empirical analysis of spam marketing conversion," in *Proceedings of the 2008 ACM conference on computer and communications security, CCS 2008, alexandria, virginia, USA, october 27-31, 2008*, 2008, pp. 3–14.

[6] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on human factors in computing systems*, ACM, 2006, pp. 581–590.

CyBOK Wiki
(as implemented)

CyBOK PDF

REFERENCES

- [1] M. McGuire and S. Dowling, "Cyber crime: A review of the evidence," *Summary of Key Findings and Implications. Home Office Research Report*, vol. 75, 2013.
- [2] N. E. Willard, *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research Press, 2007.
- [3] H. Glickman, "The Nigerian '419' advance fee scams: prank or peril?" *Canadian Journal of African Studies/La Revue Canadienne Des Études Africaines*, vol. 39, no. 3, pp. 460–489, 2005.
- [4] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *international Conference on World Wide Web (WWW)*. ACM, 2013, pp. 213–224.
- [5] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: an empirical analysis of spam marketing conversion," in *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*, 2008, pp. 3–14.
- [6] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 581–590.
- [7] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: analysis of a botnet takeover," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2009, pp. 635–647.

References [edit]

1. [↑](#) [1.0](#) [1.1](#) [1.2](#) McGuire, Mike and Dowling, Samantha, *Cyber crime: A review of the evidence* (2013)
2. [↑](#) [2.0](#) [2.1](#) Willard, Nancy E. *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress* (2007)
3. [↑](#) [3.0](#) [3.1](#) [3.2](#) Glickman, Harvey, *The (Nigerian) '419 advance fee scams: prank or peril?* (2005)
4. [↑](#) [4.0](#) [4.1](#) [4.2](#) [4.3](#) Christin, Nicolas, *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace* (2013)
5. [↑](#) [5.0](#) [5.1](#) [5.2](#) Chris Kanich and Christian Kreibich and Kirill Levchenko and Brandon Enright and Geoffrey M. Voelker and Vern Paxson and Stefan Savage, *Spamalytics: an empirical analysis of spam marketing conversion* (2008)
6. [↑](#) [6.0](#) [6.1](#) [6.2](#) Dhamija, Rachna and Tygar, J Doug and Hearst, Marti, *Why phishing works* (2006)
7. [↑](#) [7.0](#) [7.1](#) [7.2](#) [7.3](#) [7.4](#) [7.5](#) [7.6](#) Stone-Gross, Brett and Cova, Marco and Cavallaro, Lorenzo and Gilbert, Bob and Szydowski, Martin and Kemmerer, Richard and Kruegel, Christopher and Vigna, Giovanni
51. [↑](#) [51.0](#) [51.1](#) [51.2](#) [51.3](#) [51.4](#) [51.5](#) [51.6](#) [51.7](#) [51.8](#) [51.9](#) [51.10](#) [51.11](#) [51.12](#) [51.13](#) [51.14](#) [51.15](#) [51.16](#) [51.17](#) [51.18](#) [51.19](#) [51.20](#) [51.21](#) [51.22](#) [51.23](#) [51.24](#) [51.25](#) [51.26](#) [51.27](#) [51.28](#) [51.29](#) [51.30](#) [51.31](#) [51.32](#) [51.33](#) [51.34](#) [51.35](#) [51.36](#) [51.37](#) [51.38](#) [51.39](#) [51.40](#) [51.41](#) [51.42](#) [51.43](#) [51.44](#) [51.45](#) [51.46](#) [51.47](#) [51.48](#) [51.49](#) [51.50](#) [51.51](#) [51.52](#) [51.53](#) [51.54](#) [51.55](#) [51.56](#) [51.57](#) [51.58](#) [51.59](#) [51.60](#) [51.61](#) [51.62](#) [51.63](#) [51.64](#) [51.65](#) [51.66](#) [51.67](#) [51.68](#) [51.69](#) [51.70](#) [51.71](#) [51.72](#) [51.73](#) [51.74](#) [51.75](#) [51.76](#) [51.77](#) [51.78](#) [51.79](#) [51.80](#) [51.81](#) [51.82](#) [51.83](#) [51.84](#) [51.85](#) [51.86](#) [51.87](#) [51.88](#) [51.89](#) [51.90](#) [51.91](#) [51.92](#) [51.93](#) [51.94](#) [51.95](#) [51.96](#) [51.97](#) [51.98](#) [51.99](#) [51.100](#) [51.101](#) [51.102](#) [51.103](#) [51.104](#) [51.105](#) [51.106](#) [51.107](#) [51.108](#) [51.109](#) [51.110](#) [51.111](#) [51.112](#) [51.113](#) [51.114](#) [51.115](#) [51.116](#) [51.117](#) [51.118](#) [51.119](#) [51.120](#) [51.121](#) [51.122](#) [51.123](#) [51.124](#) [51.125](#) [51.126](#) [51.127](#) [51.128](#) [51.129](#) [51.130](#) [51.131](#) [51.132](#) [51.133](#) [51.134](#) [51.135](#) [51.136](#) [51.137](#) [51.138](#) [51.139](#) [51.140](#) [51.141](#) [51.142](#) [51.143](#) [51.144](#) [51.145](#) [51.146](#) [51.147](#) [51.148](#) [51.149](#) [51.150](#) [51.151](#) [51.152](#) [51.153](#) [51.154](#) [51.155](#) [51.156](#) [51.157](#) [51.158](#) [51.159](#) [51.160](#) [51.161](#) [51.162](#) [51.163](#) [51.164](#) [51.165](#) [51.166](#) [51.167](#) [51.168](#) [51.169](#) [51.170](#) [51.171](#) [51.172](#) [51.173](#) [51.174](#) [51.175](#) [51.176](#) [51.177](#) [51.178](#) [51.179](#) [51.180](#) [51.181](#) [51.182](#) [51.183](#) [51.184](#) [51.185](#) [51.186](#) [51.187](#) [51.188](#) [51.189](#) [51.190](#) [51.191](#) [51.192](#) [51.193](#) [51.194](#) [51.195](#) [51.196](#) [51.197](#) [51.198](#) [51.199](#) [51.200](#) [51.201](#) [51.202](#) [51.203](#) [51.204](#) [51.205](#) [51.206](#) [51.207](#) [51.208](#) [51.209](#) [51.210](#) [51.211](#) [51.212](#) [51.213](#) [51.214](#) [51.215](#) [51.216](#) [51.217](#) [51.218](#) [51.219](#) [51.220](#) [51.221](#) [51.222](#) [51.223](#) [51.224](#) [51.225](#) [51.226](#) [51.227](#) [51.228](#) [51.229](#) [51.230](#) [51.231](#) [51.232](#) [51.233](#) [51.234](#) [51.235](#) [51.236](#) [51.237](#) [51.238](#) [51.239](#) [51.240](#) [51.241](#) [51.242](#) [51.243](#) [51.244](#) [51.245](#) [51.246](#) [51.247](#) [51.248](#) [51.249](#) [51.250](#) [51.251](#) [51.252](#) [51.253](#) [51.254](#) [51.255](#) [51.256](#) [51.257](#) [51.258](#) [51.259](#) [51.260](#) [51.261](#) [51.262](#) [51.263](#) [51.264](#) [51.265](#) [51.266](#) [51.267](#) [51.268](#) [51.269](#) [51.270](#) [51.271](#) [51.272](#) [51.273](#) [51.274](#) [51.275](#) [51.276](#) [51.277](#) [51.278](#) [51.279](#) [51.280](#) [51.281](#) [51.282](#) [51.283](#) [51.284](#) [51.285](#) [51.286](#) [51.287](#) [51.288](#) [51.289](#) [51.290](#) [51.291](#) [51.292](#) [51.293](#) [51.294](#) [51.295](#) [51.296](#) [51.297](#) [51.298](#) [51.299](#) [51.300](#) [51.301](#) [51.302](#) [51.303](#) [51.304](#) [51.305](#) [51.306](#) [51.307](#) [51.308](#) [51.309](#) [51.310](#) [51.311](#) [51.312](#) [51.313](#) [51.314](#) [51.315](#) [51.316](#) [51.317](#) [51.318](#) [51.319](#) [51.320](#) [51.321](#) [51.322](#) [51.323](#) [51.324](#) [51.325](#) [51.326](#) [51.327](#) [51.328](#) [51.329](#) [51.330](#) [51.331](#) [51.332](#) [51.333](#) [51.334](#) [51.335](#) [51.336](#) [51.337](#) [51.338](#) [51.339](#) [51.340](#) [51.341](#) [51.342](#) [51.343](#) [51.344](#) [51.345](#) [51.346](#) [51.347](#) [51.348](#) [51.349](#) [51.350](#) [51.351](#) [51.352](#) [51.353](#) [51.354](#) [51.355](#) [51.356](#) [51.357](#) [51.358](#) [51.359](#) [51.360](#) [51.361](#) [51.362](#) [51.363](#) [51.364](#) [51.365](#) [51.366](#) [51.367](#) [51.368](#) [51.369](#) [51.370](#) [51.371](#) [51.372](#) [51.373](#) [51.374](#) [51.375](#) [51.376](#) [51.377](#) [51.378](#) [51.379](#) [51.380](#) [51.381](#) [51.382](#) [51.383](#) [51.384](#) [51.385](#) [51.386](#) [51.387](#) [51.388](#) [51.389](#) [51.390](#) [51.391](#) [51.392](#) [51.393](#) [51.394](#) [51.395](#) [51.396](#) [51.397](#) [51.398](#) [51.399](#) [51.400](#) [51.401](#) [51.402](#) [51.403](#) [51.404](#) [51.405](#) [51.406](#) [51.407](#) [51.408](#) [51.409](#) [51.410](#) [51.411](#) [51.412](#) [51.413](#) [51.414](#) [51.415](#) [51.416](#) [51.417](#) [51.418](#) [51.419](#) [51.420](#) [51.421](#) [51.422](#) [51.423](#) [51.424](#) [51.425](#) [51.426](#) [51.427](#) [51.428](#) [51.429](#) [51.430](#) [51.431](#) [51.432](#) [51.433](#) [51.434](#) [51.435](#) [51.436](#) [51.437](#) [51.438](#) [51.439](#) [51.440](#) [51.441](#) [51.442](#) [51.443](#) [51.444](#) [51.445](#) [51.446](#) [51.447](#) [51.448](#) [51.449](#) [51.450](#) [51.451](#) [51.452](#) [51.453](#) [51.454](#) [51.455](#) [51.456](#) [51.457](#) [51.458](#) [51.459](#) [51.460](#) [51.461](#) [51.462](#) [51.463](#) [51.464](#) [51.465](#) [51.466](#) [51.467](#) [51.468](#) [51.469](#) [51.470](#) [51.471](#) [51.472](#) [51.473](#) [51.474](#) [51.475](#) [51.476](#) [51.477](#) [51.478](#) [51.479](#) [51.480](#) [51.481](#) [51.482](#) [51.483](#) [51.484](#) [51.485](#) [51.486](#) [51.487](#) [51.488](#) [51.489](#) [51.490](#) [51.491](#) [51.492](#) [51.493](#) [51.494](#) [51.495](#) [51.496](#) [51.497](#) [51.498](#) [51.499](#) [51.500](#) [51.501](#) [51.502](#) [51.503](#) [51.504](#) [51.505](#) [51.506](#) [51.507](#) [51.508](#) [51.509](#) [51.510](#) [51.511](#) [51.512](#) [51.513](#) [51.514](#) [51.515](#) [51.516](#) [51.517](#) [51.518](#) [51.519](#) [51.520](#) [51.521](#) [51.522](#) [51.523](#) [51.524](#) [51.525](#) [51.526](#) [51.527](#) [51.528](#) [51.529](#) [51.530](#) [51.531](#) [51.532](#) [51.533](#) [51.534](#) [51.535](#) [51.536](#) [51.537](#) [51.538](#) [51.539](#) [51.540](#) [51.541](#) [51.542](#) [51.543](#) [51.544](#) [51.545](#) [51.546](#) [51.547](#) [51.548](#) [51.549](#) [51.550](#) [51.551](#) [51.552](#) [51.553](#) [51.554](#) [51.555](#) [51.556](#) [51.557](#) [51.558](#) [51.559](#) [51.560](#) [51.561](#) [51.562](#) [51.563](#) [51.564](#) [51.565](#) [51.566](#) [51.567](#) [51.568](#) [51.569](#) [51.570](#) [51.571](#) [51.572](#) [51.573](#) [51.574](#) [51.575](#) [51.576](#) [51.577](#) [51.578](#) [51.579](#) [51.580](#) [51.581](#) [51.582](#) [51.583](#) [51.584](#) [51.585](#) [51.586](#) [51.587](#) [51.588](#) [51.589](#) [51.590](#) [51.591](#) [51.592](#) [51.593](#) [51.594](#) [51.595](#) [51.596](#) [51.597](#) [51.598](#) [51.599](#) [51.600](#) [51.601](#) [51.602](#) [51.603](#) [51.604](#) [51.605](#) [51.606](#) [51.607](#) [51.608](#) [51.609](#) [51.610](#) [51.611](#) [51.612](#) [51.613](#) [51.614](#) [51.615](#) [51.616](#) [51.617](#) [51.618](#) [51.619](#) [51.620](#) [51.621](#) [51.622](#) [51.623](#) [51.624](#) [51.625](#) [51.626](#) [51.627](#) [51.628](#) [51.629](#) [51.630](#) [51.631](#) [51.632](#) [51.633](#) [51.634](#) [51.635](#) [51.636](#) [51.637](#) [51.638](#) [51.639](#) [51.640](#) [51.641](#) [51.642](#) [51.643](#) [51.644](#) [51.645](#) [51.646](#) [51.647](#) [51.648](#) [51.649](#) [51.650](#) [51.651](#) [51.652](#) [51.653](#) [51.654](#) [51.655](#) [51.656](#) [51.657](#) [51.658](#) [51.659](#) [51.660](#) [51.661](#) [51.662](#) [51.663](#) [51.664](#) [51.665](#) [51.666](#) [51.667](#) [51.668](#) [51.669](#) [51.670](#) [51.671](#) [51.672](#) [51.673](#) [51.674](#) [51.675](#) [51.676](#) [51.677](#) [51.678](#) [51.679](#) [51.680](#) [51.681](#) [51.682](#) [51.683](#) [51.684](#) [51.685](#) [51.686](#) [51.687](#) [51.688](#) [51.689](#) [51.690](#) [51.691](#) [51.692](#) [51.693](#) [51.694](#) [51.695](#) [51.696](#) [51.697](#) [51.698](#) [51.699](#) [51.700](#) [51.701](#) [51.702](#) [51.703](#) [51.704](#) [51.705](#) [51.706](#) [51.707](#) [51.708](#) [51.709](#) [51.710](#) [51.711](#) [51.712](#) [51.713](#) [51.714](#) [51.715](#) [51.716](#) [51.717](#) [51.718](#) [51.719](#) [51.720](#) [51.721](#) [51.722](#) [51.723](#) [51.724](#) [51.725](#) [51.726](#) [51.727](#) [51.728](#) [51.729](#) [51.730](#) [51.731](#) [51.732](#) [51.733](#) [51.734](#) [51.735](#) [51.736](#) [51.737](#) [51.738](#) [51.739](#) [51.740](#) [51.741](#) [51.742](#) [51.743](#) [51.744](#) [51.745](#) [51.746](#) [51.747](#) [51.748](#) [51.749](#) [51.750](#) [51.751](#) [51.752](#) [51.753](#) [51.754](#) [51.755](#) [51.756](#) [51.757](#) [51.758](#) [51.759](#) [51.760](#) [51.761](#) [51.762](#) [51.763](#) [51.764](#) [51.765](#) [51.766](#) [51.767](#) [51.768](#) [51.769](#) [51.770](#) [51.771](#) [51.772](#) [51.773](#) [51.774](#) [51.775](#) [51.776](#) [51.777](#) [51.778](#) [51.779](#) [51.780](#) [51.781](#) [51.782](#) [51.783](#) [51.784](#) [51.785](#) [51.786](#) [51.787](#) [51.788](#) [51.789](#) [51.790](#) [51.791](#) [51.792](#) [51.793](#) [51.794](#) [51.795](#) [51.796](#) [51.797](#) [51.798](#) [51.799](#) [51.800](#) [51.801](#) [51.802](#) [51.803](#) [51.804](#) [51.805](#) [51.806](#) [51.807](#) [51.808](#) [51.809](#) [51.810](#) [51.811](#) [51.812](#) [51.813](#) [51.814](#)

CyBOK PDF

CONTENT

1 MATHEMATICS

[3, c8–c9, App B][4, c1–c5]

Cryptography is inherently mathematical in nature, the reader is therefore going to be assumed to be familiar with a number of concepts. A good textbook to cover the basics needed, and more, is that of Galbraith [5].

Before proceeding we will set up some notation: The ring of integers is denoted by \mathbb{Z} , whilst the fields of rational, real and complex numbers are denoted by \mathbb{Q} , \mathbb{R} and \mathbb{C} . The ring of integers modulo N will be denoted by $\mathbb{Z}/N\mathbb{Z}$, when N is a prime p this is a finite field often denoted by \mathbb{F}_p . The set of invertible elements will be written $(\mathbb{Z}/N\mathbb{Z})^*$ or \mathbb{F}_p^* . An RSA modulus N will denote an integer N , which is the product of two (large) prime factors $N = p \cdot q$.

Finite abelian groups of prime order q are also a basic construct. These are either written multiplicatively, in which case an element is written as g^x for some $x \in \mathbb{Z}/q\mathbb{Z}$; when written additively an element can be written as $[x] \cdot P$. The element g (in the multiplicative case) and P (in the additive case) is called the generator.

The standard example of finite abelian groups of prime order used in cryptography are elliptic curves. An elliptic curve over a finite field \mathbb{F}_p is the set of solutions (X, Y) to an equation of the form

$$E : Y^2 = X^3 + A \cdot X + B$$

where A and B are fixed constants. Such a set of solutions, plus a special point at infinity denoted by \mathcal{O} , form a finite abelian group denoted by $E(\mathbb{F}_p)$. The group law is a classic law dating back to Newton and Fermat called the chord-tangent process. When A and B are selected carefully one can ensure that the size of $E(\mathbb{F}_p)$ is a prime q . This will be important later in Section 2.3 to ensure the discrete logarithm problem in the elliptic curve is hard.

CyBOK Wiki

Mathematics

Page Discussion

Read Edit View history Tools ▾

(Redirected from [Crypto:sec:math](#))

Parent chapter: [\[Cryptography\]](#)

[1, pp. c8–c9], App B[2, pp. c1–c5] Cryptography is inherently mathematical in nature, the reader is therefore going to be assumed to be familiar with a number of concepts. A good textbook to cover the basics needed, and more, is that of Galbraith [3].

Before proceeding we will set up some notation: The ring of integers is denoted by \mathbb{Z} , whilst the fields of rational, real and complex numbers are denoted by \mathbb{Q} , \mathbb{R} and \mathbb{C} . The ring of integers modulo N will be denoted by $\mathbb{Z}/N\mathbb{Z}$, when N is a prime p this is a finite field often denoted by \mathbb{F}_p . The set of invertible elements will be written $(\mathbb{Z}/N\mathbb{Z})^*$ or \mathbb{F}_p^* . An RSA modulus N will denote an integer N , which is the product of two (large) prime factors $N = p \cdot q$.

Finite abelian groups of prime order q are also a basic construct. These are either written multiplicatively, in which case an element is written as g^x for some $x \in \mathbb{Z}/q\mathbb{Z}$; when written additively an element can be written as $[x] \cdot P$. The element g (in the multiplicative case) and P (in the additive case) is called the generator.

The standard example of finite abelian groups of prime order used in cryptography are elliptic curves. An elliptic curve over a finite field \mathbb{F}_p is the set of solutions (X, Y) to an equation of the form

$$E : Y^2 = X^3 + A \cdot X + B$$

where A and B are fixed constants. Such a set of solutions, plus a special point at infinity denoted by \mathcal{O} , form a finite abelian group denoted by $E(\mathbb{F}_p)$. The group law is a classic law dating back to Newton and Fermat called the chord-tangent process. When A and B are selected carefully one can ensure that the size of $E(\mathbb{F}_p)$ is a prime q . This will be important later in Section [\[crypto:sec:hardproblems\]](#) to ensure the discrete logarithm problem in the elliptic curve is hard.

CyBOK PDF

CyBOK Wiki

The Cyber Security Body Of Knowledge
www.cybok.org

CyBOK

CROSS REFERENCE OF TOPICS VS REFERENCE MATERIAL

Sections	Cites
1 A Characterisation of Adversaries	
Cyber-enabled and cyber-dependent crimes	[1]
Interpersonal offenders	[2, 28, 31, 33, 34]
Cyber-enabled organised criminals	[3, 4, 43]
Cyber-dependent organised criminals	[5, 6, 7, 69, 70, 77, 79]
Hacktivists	[8, 18, 86]
State actors	[9, 10, 93, 96]
2 The Elements of a Malicious Operation	
Affiliate programmes	[56, 99]
Infection vectors	[15, 100]
Infrastructure	[101, 114, 115]
Specialised services	[103, 102]
Human services	[67, 119, 124, 120]
Payment methods	[55, 104, 105]
3 Models to Understand Malicious Operations	
Attack trees	[128]
Environmental criminology	[130, 131, 132]
Modelling the underground economy as a flow of capital	[13]
Attack attribution	[133]

Cross Reference of Topics vs Reference Material [\[edit\]](#)

Sections	Cites
Cyber-enabled and cyber-dependent crimes	[30]
Interpersonal offenders	[31], [32], [33], [34], [35]
Cyber-enabled organised criminals	[20], [23], [36]
Cyber-dependent organised criminals	[17], [37], [38], [39], [40], [41], [42]
Hacktivists	[43], [44], [45]
State actors	[46], [47], [48], [49]
Affiliate programmes	[25], [50]
Infection vectors	[51], [52]
Infrastructure	[53], [54], [55]
Specialised services	[56], [57]
Human services	[58], [59], [60], [61]
Payment methods	[62], [63], [64]
Attack trees	[1]
Environmental criminology	[3], [4], [5]
Modelling the underground economy as a flow of capital	[6]
Attack attribution	[7]

Feasible, but

- open questions – technical, editorial
- some technical challenges
- lots of work ahead

Opportunities and questions

CyBOK is linked with indices, acronyms, glossary

- 2757 \index{} elements in one KA
- Opportunities?
 - Dedicated pages, with backlinks
 - recommendations,
 - smart search,
 - topic browser

CyBOK is linked data.

Index

1995 Directive, 80
2-safety hyperproperty, 431, 432
2D stepper, 698
2G network, 763, 764
3-D Secure, 678
32-bit, 366, 376, 377
3G network, 763, 764
4-layer Internet protocol suite, 651
419 scam, 228
4G network, 763, 764
4chan, 226, 248
4chan's Politically Incorrect board, 226, 248
5G network, 442, 638, 678, 764
64-bit, 377, 378, 455
6LoWPAN, 711
802.1X, 665–667, 669, 711, 748, 751, 756

A5/1 stream cipher, 600
A5/2 stream cipher, 600
AAMP7G, 440
abelian group, 323, 327, 340
absolute positioning, 544
absolute URL, 528
abstract interpretation, 514
abstract syntax tree, 221
abstraction, 5, 7, 11, 295, 299, 301–305, 310, 314, 316, 426, 427, 429, 430, 436–438, 440, 444, 445, 448, 457–459, 504–506, 512–514

abuse, 226, 561, 567, 568, 582, 711, 733
abusive language, 226
accelerometer, 720, 731, 759, 760
accept header, 528
acceptability, 21–24, 36, 40, 146, 148
acceptable security, 11, 12
acceptable use policy, 82, 101
access control, 8, 14, 172, 174, 188, 190, 272, 279, 368–374, 389, 394, 397, 398, 411, 414, 416–418, 426, 428, 451, 452, 461, 462, 466–478, 480, 484, 489, 490, 493, 494, 504, 518, 524, 525, 533–535, 538, 546, 548, 552, 569, 629, 650, 665, 669, 671, 674–677, 694, 703, 704, 718, 721, 725, 738, 739, 742, 743, 745, 759, 761
access control capabilities, 372–374, 380, 390, 469
access control list, 371–373, 469, 475
access control logic, 475, 504
access control matrix, 461, 469
access control policy, 371, 461, 462, 518, 534, 548, 689
access decision, 563
access management, 9
access matrix, 372
access operations, 468, 474
access pattern, 216, 348, 454, 505
access permissions, 302, 524, 530, 533–535, 545, 551, 553, 555

How to display CyBOK's structure in MediaWiki and improve navigation?

notes have been used to suggest potential future legal developments, subjects worthy of further study, or to provide other comments.⁸

KA Law and Regulation | July 2021 Page 4

The Cyber Security Body Of Knowledge CyBOK
www.cybok.org

CONTENT

1 INTRODUCTORY PRINCIPLES OF LAW AND LEGAL RESEARCH

Cyber security practitioners and researchers come from an incredibly wide array of educational backgrounds. Experience teaching legal and regulatory subjects to cyber security post-graduate students, and providing legal advice to cyber security practitioners, suggests that much of this knowledge area's content will be novel to those whose education is based in science, technology, engineering, mathematics, many social sciences, and many of the humanities. These introductory observations are offered as an aid for those who are approaching the subject without significant experience.

1.1 The nature of law and legal analysis

Although the reader is assumed to have some degree of familiarity with the process of law making and law enforcement, a review of some of the most common sources of law should

3 Law & Regulation	49
Introduction	50
3.1 Introductory principles of law and legal research	52
3.1.1 The nature of law and legal analysis	52
3.1.2 Applying law to cyberspace and information technologies	54
3.1.3 Distinguishing criminal and civil law	55
3.1.3.1 Criminal law	55
3.1.3.2 Civil (non-criminal) law	55
3.1.3.3 One act: two types of liability & two courts	56
3.1.4 The nature of evidence and proof	56
3.1.5 A more holistic approach to legal risk analysis	57
3.2 Jurisdiction	59
3.2.1 Territorial jurisdiction	59
3.2.2 Personal jurisdiction	60

- Breadcrumbs
- Sidebar, infobox
- Parent, children, sibling links
- How closely do we replicate?

Introductory principles of law and legal research

Page Discussion Read Edit View history Tools ▾

Parent section: [\[Law and Regulation\]](#)

Cyber security practitioners and researchers come from an incredibly wide array of educational backgrounds. Experience teaching legal and regulatory subjects to cyber security post-graduate students, and providing legal advice to cyber security practitioners, suggests that much of this knowledge area's content will be novel to those whose education is based in science, technology, engineering, mathematics, many social sciences, and many of the humanities. These introductory observations are offered as an aid for those who are approaching the subject without significant experience.

Subsections [\[edit\]](#)

- [\[The nature of law and legal analysis\]](#)
- [\[Applying law to cyberspace and information technologies\]](#)
- [\[Distinguishing criminal and civil law\]](#)
- [\[The nature of evidence and proof\]](#)
- [\[A more holistic approach to legal risk analysis\]](#)

Changing the LaTeX source

Pairing (sub)section **titles** and **labels** is difficult

Needed for cross-reference hyperlinks between (sub)sections

LaTeX codebase should be standardized

```
\topic{A Characterisation of Adversaries  
  \label{sec:ab-taxonomy}  
}
```

Larger implications:

- Existing codebase
- Work of authors, editors effected

inconsistent code title and label use

```
\topic{The Elements of a Malicious Operation}  
\label{sect:elements}
```

```
\subtopic{Syntax of Basic Schemes}  
\index{cryptographic syntax}
```

```
\topic{Information-theoretically Secure Constructions}  
\index{information-theoretic security}  
\index{information theory}  
\label{crypto:sec:IT}
```

```
\subtopic{Message Authentication Codes}  
\index{authentication}  
\label{sec:crypto:MAC}
```

```
\label{fig:CBC}
```

Further learnings

Technical considerations for beyond proof-of-concept

- Tackling LaTeX expressions not converted correctly by Pandoc
- Manual tasks in the automated conversion pipeline
- KA-specific functionality
- Math
- Illustrations
- Misc. Todos

Open questions

- Which subsections should be segmented into Wiki articles?
- How to display section titles?
- LaTeX metadata to MediaWiki
- Versioning

Next steps

- Feasibility study on all 22 KAs (*funding secured*)
- Service design:
 - Wiki is not just a clone of PDF:
 - a new service with new functions, use cases, risks, and limitations.
 - a chance to rethink what CyBOK is, and what it may become.

Thank you!

Lőrinc Thurnay *(Lawrence)*
research associate
Center for e-Governance

loerinc.thurnay@donau-uni.ac.at



University for
Continuing
Education KREMS



CyBOK Wiki:
feasibility study
Documentation

Lőrinc Thurnay | University for Continuing
Education KREMS



https://www.cybok.org/media/downloads/CyBOK_Wiki_feasibility_study_finalreport.pdf

Opportunities and questions

Which **(sub)sections** to segment into **Wiki articles**?

- Knowledge areas?
- Table of Content elements?
- Every subsection (even ones excluded from ToC)?
- Avoiding very short Wiki pages

11 OTHER REGULATORY MATTERS

This section will briefly address additional miscellaneous regulatory topics that a cyber security practitioner might be expected to encounter.

11.1 Industry-specific regulations and NIS Directive

A wide variety of single-industry regulators have embraced cyber security within the framework of their respective regulatory subject industries [170]. Many financial services regulators, for

diversified enough to cover
explained in Section 7.2). In
to make money and usual

Opportunities and questions

How to display section titles?

- In text references
- As titles

Numbering?

Context? (e.g.: "Section 20.8.5 Time" (KA Network Security))

PDF original	diversified enough to cover explained in Section 7.2). In to make money and usual
like PDF original	...explained in Section 7.2 ...
with number and title	...explained in Section 7.2 " A Characterisation of Adversaries "...
only title	...explained in Section " A Characterisation of Adversaries "...
removing Section prefix	...explained in " A Characterisation of Adversaries "...