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

University for Continuing Education Krems



Research interests:
- Open data applications
- Open legal data
- ML/NLP
- Cyber-security


loerinc.thurnay@donau-uni.ac.at

# 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 |

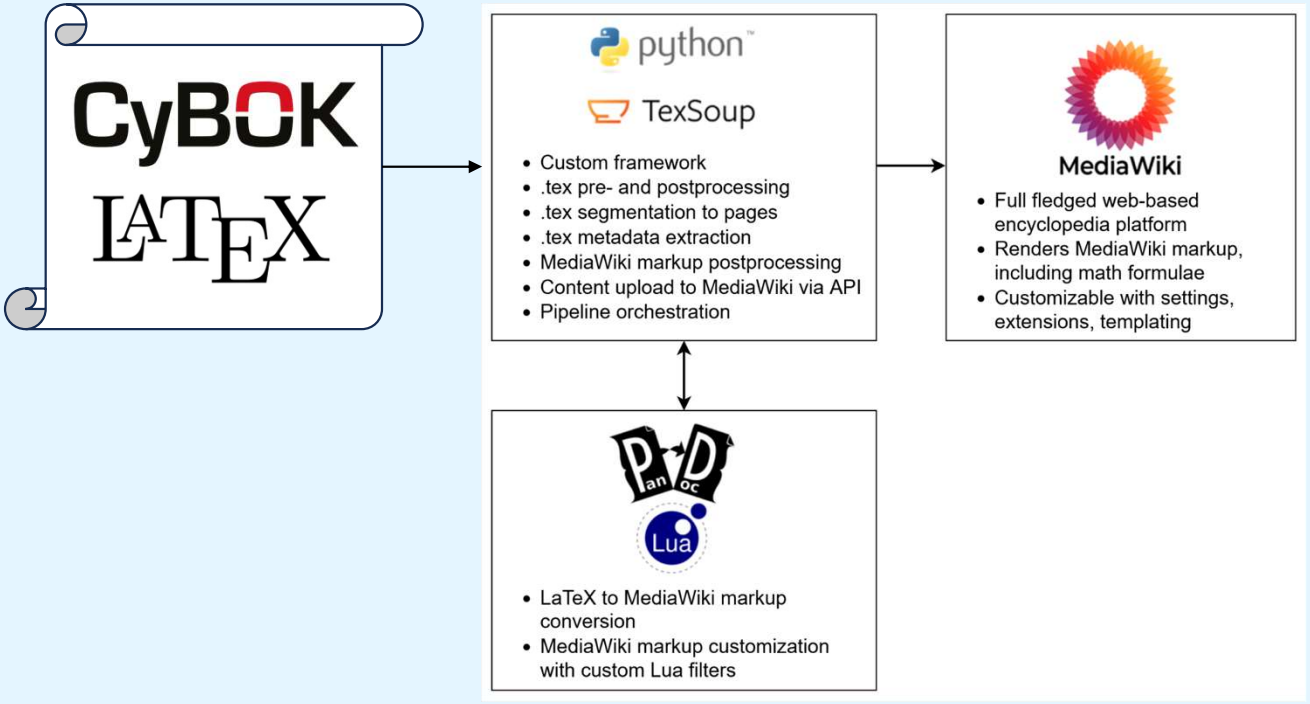
# Feasibility study

RQ: Is CyBOK Wiki technically feasible – and how?

Proof-of-concept software

Based on 3 KAs

# Software proof-of-concept

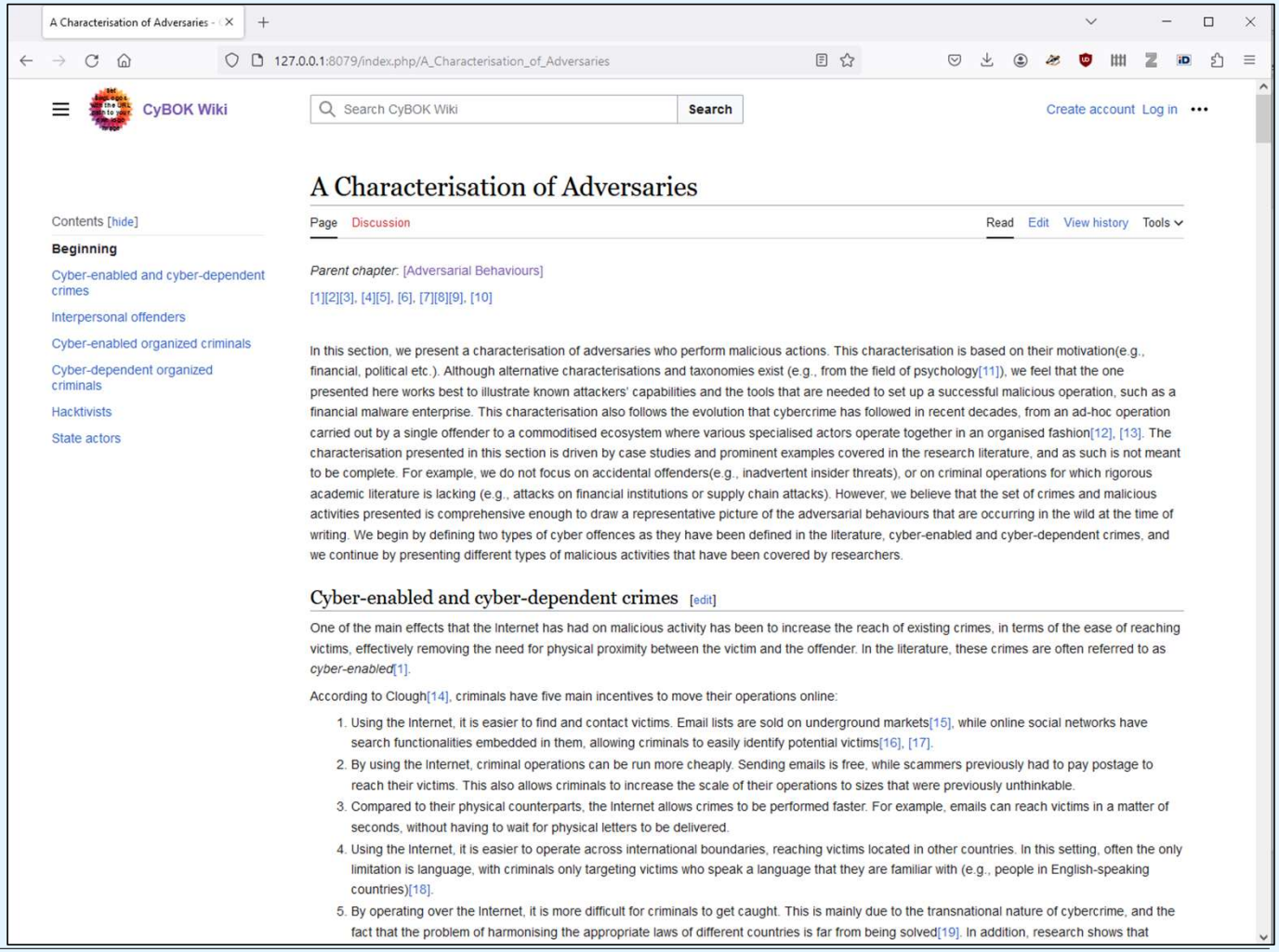



- **Segmentation**
  (sub)chapters to Wiki articles
- **Conversion**
  LaTeX code to Wiki markup
  Custom preprocessors and Pandoc
- **Publishing**
  to MediaWiki instance

# CyBOK Wiki Prototype

3 KAs into 118 Wiki pages

Not online




CyBOK

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'.

CyBOK

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**

CyBOK

# Bibliographies

**CyBOK Wiki**
(as implemented)


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

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

[3] H. Glickman, "The Nigerian '419' advance fee scams: Prank or peril?" *Canadian Journal of African Studies/La Revue C*
*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 *Internationa*
*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 c*
*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 fac*
ACM, 2006, pp. 581–590.


**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. Szydlowski, 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 Szydlowski, Martin and Kemmerer, Richard and Kruegel, Christopher and Vigna, Giovanni

51. ↑ 51.0 51.1 51.2 51.3 5 *organized cybercrim*
52. ↑ Hinde, Stephen, *Sp*
53. ↑ 53.0 53.1 McWilliam *high-rolling huckster* (2014)
54. ↑ Stringhini, Gianluca and Vigna, Giovanni *on the relations betw* (2014)
55. ↑ 55.0 55.1 55.2 55.3 5 Jordan, Grant and W Brian and Voelker, G Kirill, *Pharmaleaks: U pharmaceutical affilia*
56. ↑ 56.0 56.1 Samossei *should you care* (20
57. ↑ Spirin, Nikita and H *principles and algori*


**CyBOK Wiki to-be**
(with native MW citation rendering)

CyBOK

## CyBOK PDF

The Cyber Security Body Of Knowledge
www.cybok.org

CyBOK

### 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 $N = p \cdot q$.

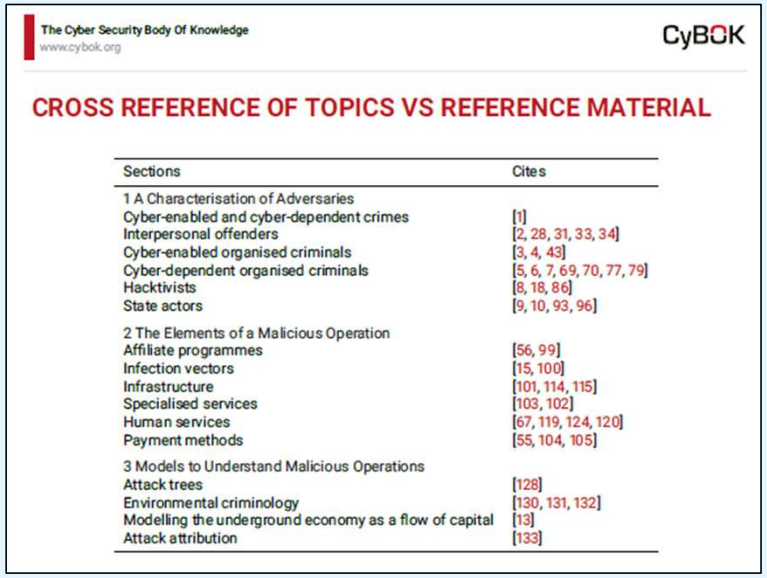
Finite abelian groups of prime order $q$ are also a basic construct. These are either written multiplicatively, in which case an element is written as $g^x$ for some $x \in \mathbb{Z}/q\mathbb{Z}$; when written additively an element can be written as $[x] \cdot P$. The element $g$(in the multiplicative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



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] |

CyBOK Wiki

## 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

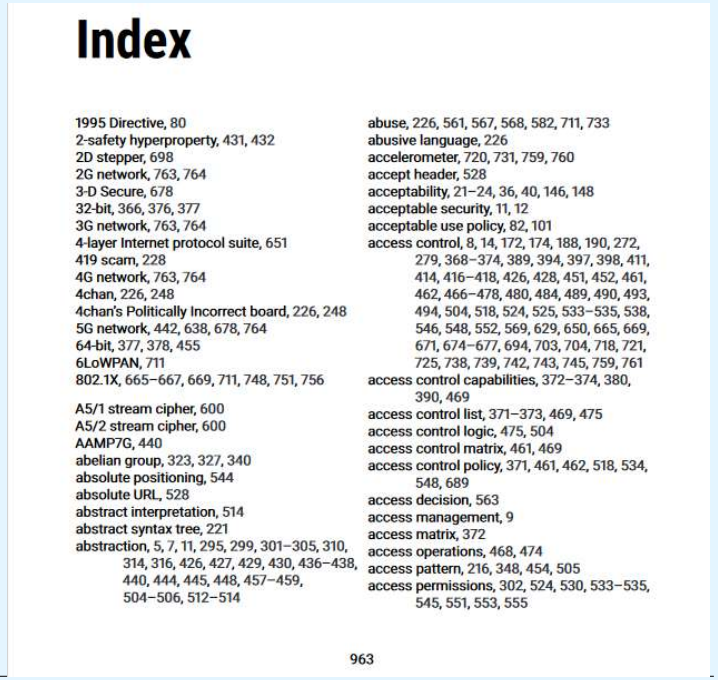
- open questions – technical, editorial
- some technical challenges
- lots of work ahead

# 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.

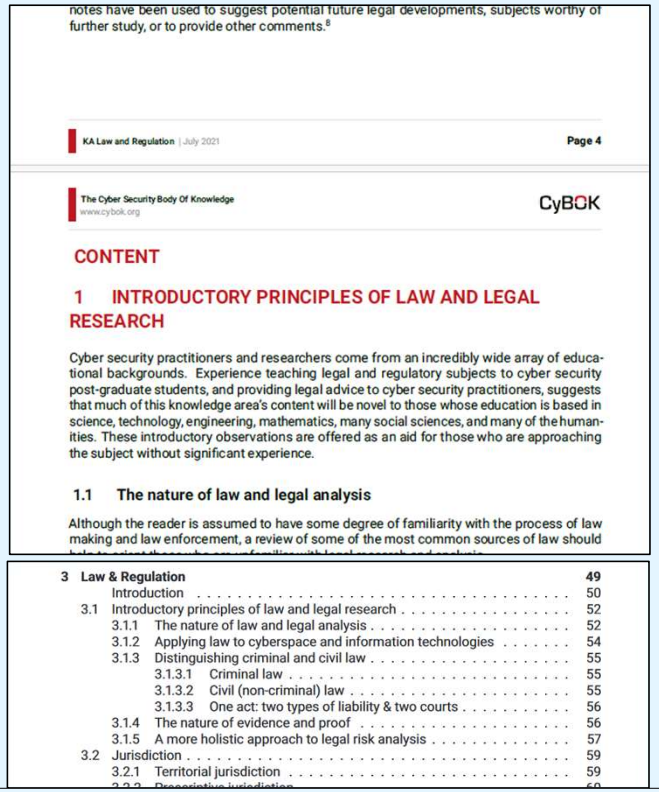


## Index



963

# 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.[6]

KA Law and Regulation | July 2021 Page 4

The Cyber Security Body Of Knowledge
www.cybok.org

CyBOK

CONTENT

1 INTRODUCTORY PRINCIPLES OF LAW AND LEGAL RESEARCH

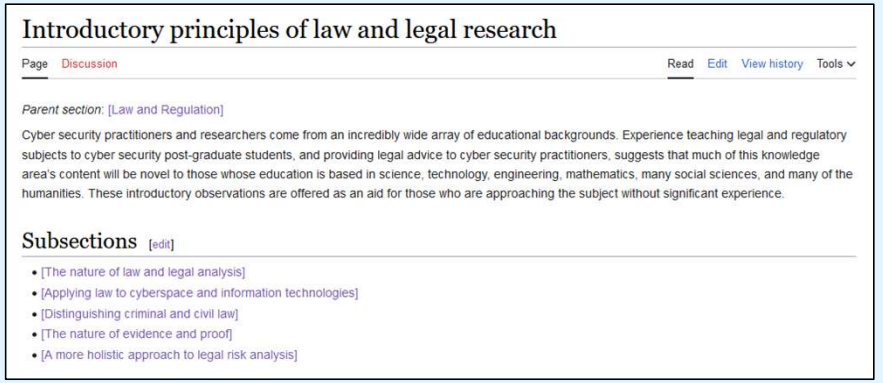
Cyber security practitioners and researchers come from an incredibly wide array of educational backgrounds. Experience teaching legal and regulatory subjects to cyber security post-graduate students, and providing legal advice to cyber security practitioners, suggests that much of this knowledge area's 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



- 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


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


# 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 |  |
| 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"... |