CyBOK

The Cyber Security Body Of Knowledge

CyBOK Wiki: Expanded Technical Feasibility Study

CyBOK Funded Project

contact@cybok.org
www.cybok.org

Hi!

Lőrinc Thurnay *(Lawrence)*
research associate
Department for E-Governance and Administration

University for Continuing Education Krems

DONAU UNIVERSITÄT KREMS

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

thurnay@protonmail.com

Motivation

- CyBOK is >1000 pages, PDF only
- Linear, but I need to browse and explore
- Could it be released as a Wiki platform?
  - Read only, no direct community contributions

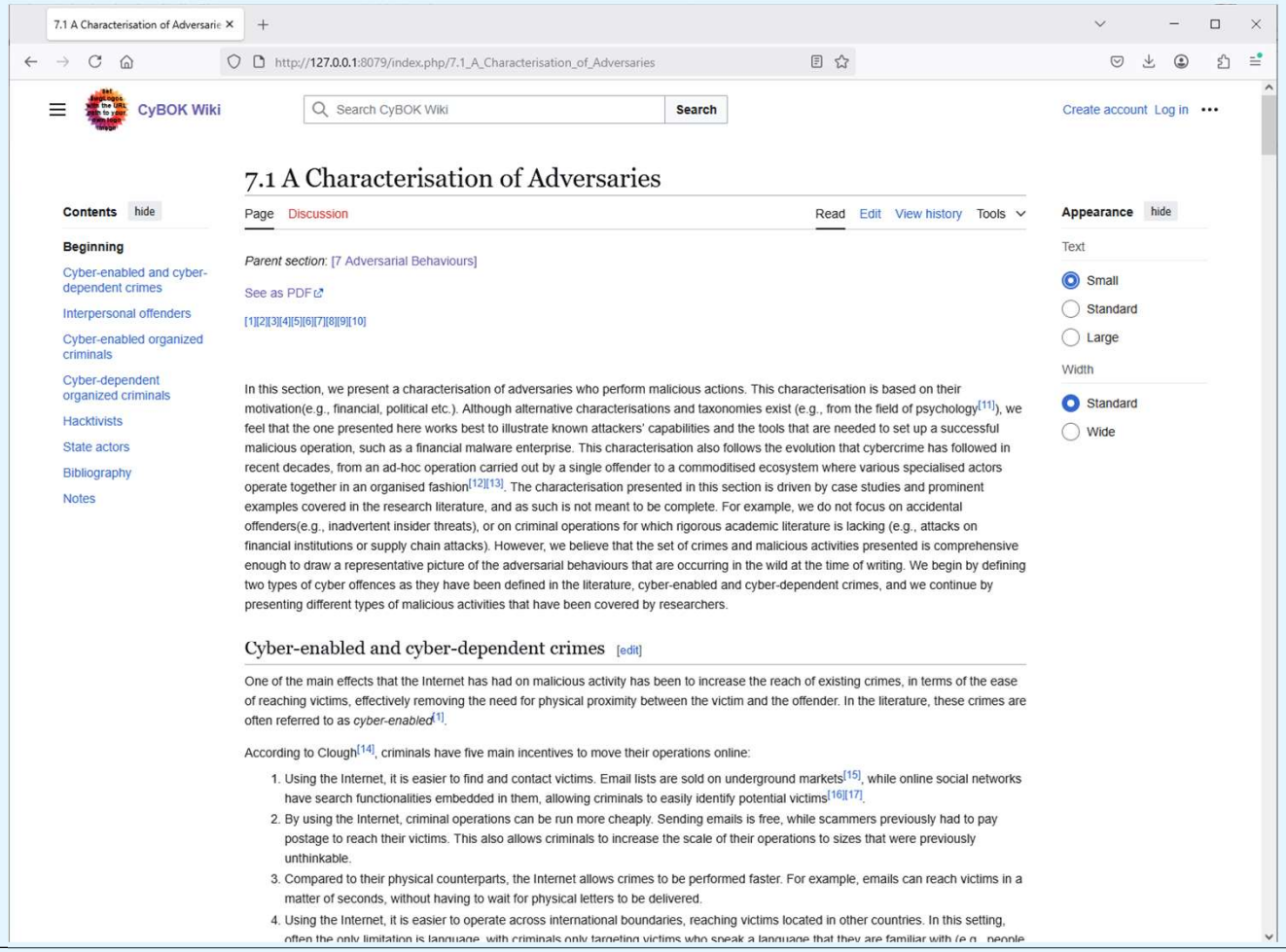
User eXperience →	search, smart recommendations, multi-tab, copy/paste
Accessibility →	responsive to screen size, screen readers
Discoverability →	SEO, links to individual (sub)sections

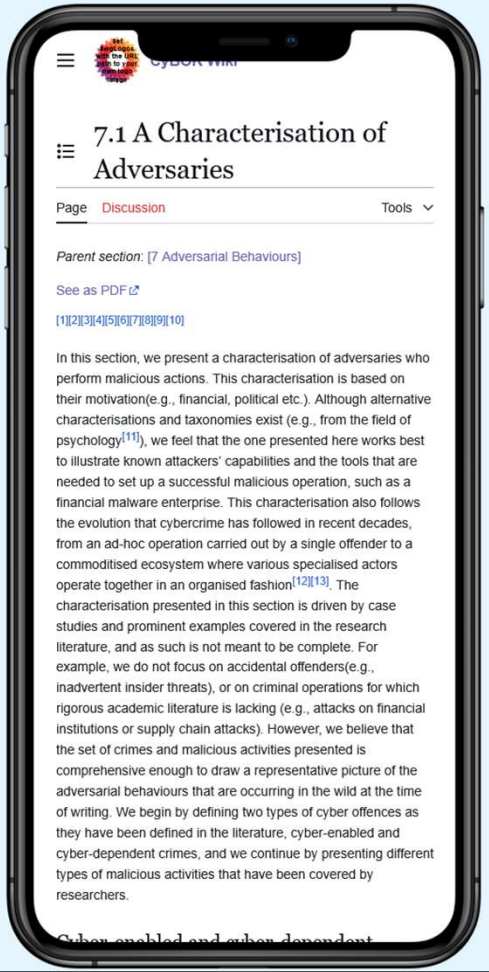
Feasibility study

- RQ: Is CyBOK Wiki technically feasible – and how?
  - Software prototype

- 1st round: 3 KAs
- 2nd roud: all 22 KAs and 3 SGs
  →full coverage, new learnings, new features implemented
  →no public release

CyBOK Wiki Prototype





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.

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'.

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].

CyBOK Wiki

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]

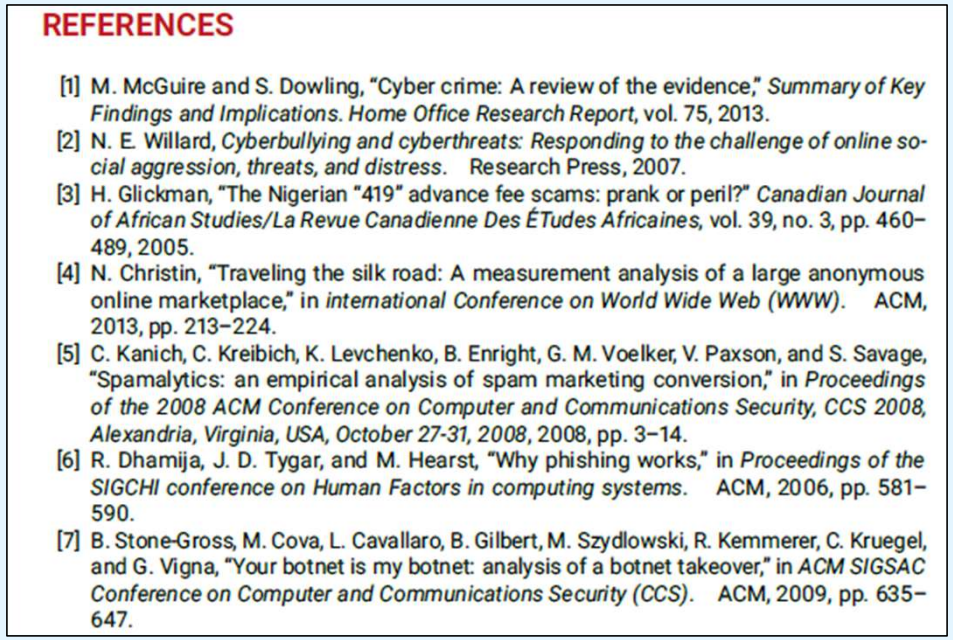
The first category that we are going to analyse is that of *interpersonal crimes*. These crimes include targeted violence and harassment, directed at either close connections (e.g., family members) or strangers. While these crimes have always existed, the Internet has made the reach of harassers and 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

Bibliographies

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.

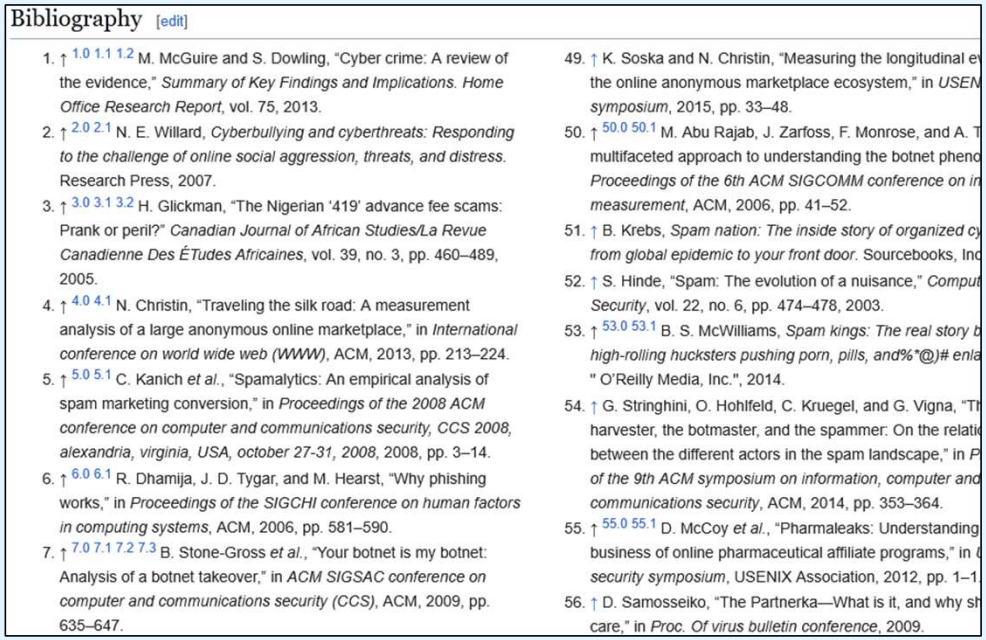
[4] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *international Conference on World Wide Web (WWW)*. ACM, 2013, pp. 213–224.

[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.

CyBOK Wiki



Bibliography [edit]

1. ↑ [1.0](#) [1.1](#) [1.2](#) 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. ↑ [2.0](#) [2.1](#) N. E. Willard, *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research Press, 2007.
3. ↑ [3.0](#) [3.1](#) [3.2](#) 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. ↑ [4.0](#) [4.1](#) 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. ↑ [5.0](#) [5.1](#) 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. ↑ [6.0](#) [6.1](#) 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. ↑ [7.0](#) [7.1](#) [7.2](#) [7.3](#) B. Stone-Gross *et al.*, "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.
49. ↑ K. Soska and N. Christin, "Measuring the longitudinal ev the online anonymous marketplace ecosystem," in *USEN symposium*, 2015, pp. 33–48.
50. ↑ [50.0](#) [50.1](#) M. Abu Rajab, J. Zarfoss, F. Monrose, and A. T multifaceted approach to understanding the botnet pheno *Proceedings of the 6th ACM SIGCOMM conference on in measurement*, ACM, 2006, pp. 41–52.
51. ↑ B. Krebs, *Spam nation: The inside story of organized cy from global epidemic to your front door*. Sourcebooks, Inc
52. ↑ S. Hinde, "Spam: The evolution of a nuisance," *Comput Security*, vol. 22, no. 6, pp. 474–478, 2003.
53. ↑ [53.0](#) [53.1](#) B. S. McWilliams, *Spam kings: The real story b high-rolling hucksters pushing porn, pills, and%*@)# enla* " O'Reilly Media, Inc.", 2014.
54. ↑ G. Stringhini, O. Hohlfeld, C. Kruegel, and G. Vigna, "Th harvester, the botmaster, and the spammer: On the relati between the different actors in the spam landscape," in *P of the 9th ACM symposium on information, computer and communications security*, ACM, 2014, pp. 353–364.
55. ↑ [55.0](#) [55.1](#) D. McCoy *et al.*, "Pharmaleaks: Understanding business of online pharmaceutical affiliate programs," in *security symposium*, USENIX Association, 2012, pp. 1–1
56. ↑ D. Samosseiko, "The Partnerka—What is it, and why sh care," in *Proc. Of virus bulletin conference*, 2009.

Formulae, displayed as browser-native MathML
Numbering, backlinks

CyBOK PDF

The Cyber Security Body Of Knowledge
www.cybok.org

CyBOK

CONTENT

10.1 MATHEMATICS

[962, c8–c9,App B][963, 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 [964].

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 10.2.3 to ensure the discrete logarithm problem in the elliptic curve is hard.

CyBOK Wiki

10.1 Mathematics

Page Discussion Read Edit View history Tools

Parent section: [10 Cryptography]

See as PDF

[1][2] 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

Illustrations, including native LaTeX figures
Acronyms

MAC [edit]

Message Authentication Code

Click here to list every page that mentions "MAC"

The following pages link to Acr:MAC:

Displaying 10 items.

View (previous 50 | next 50) (20 | 50 | 100 | 250 | 500)

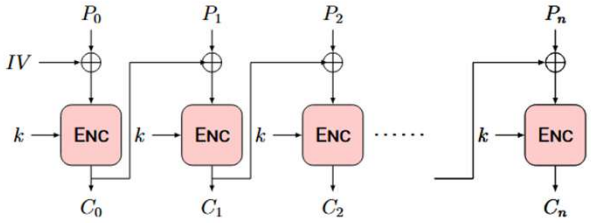
- 10.2.1 Syntax of Basic Schemes (← links | edit)
- 10.2.2 Basic Security Definitions (← links | edit)
- 10.5 Symmetric Encryption and Authentication (← links | edit)
- 10.5.1 Modes of Operation (← links | edit)
- 10.5.2 Message Authentication Codes (← links | edit)
- 10.5.3 Key Derivation and Extendable Output Functions (← links | edit)
- 10.8.1 Authentication Protocols (← links | edit)
- 20.4 Hardware support for software security at architecture level (← links | edit)
- 20.5.2 Cryptographic algorithms at RTL level (← links | edit)
- 19.3.4 Security on the Link Layer (← links | edit)

CyBOK PDF

5 SYMMETRIC ENCRYPTION AND AUTHENTICATION

[3, c3–c4][4, c13–c14]

A block cipher, such as AES or DES, does not provide an effective form of data encryption or data/entity authentication on its own. To provide such symmetric cryptographic constructions, one needs a scheme, which takes the primitive and then utilizes this in a more complex construction to provide the required cryptographic service. In the context of symmetric encryption, these are provided by modes of operation. In the case of authentication, it is provided by a MAC construction. Additionally, block ciphers are often used to take some entropy and then expand, or collapse, this into a pseudo-random stream or key; a so-called XOF (or Extendable Output Function) or KDF (or Key Derivation Function). Further details on block cipher based constructions can be found at [16], whereas further details on Sponger/Keccak based constructions can be found at [15].



CyBOK Wiki

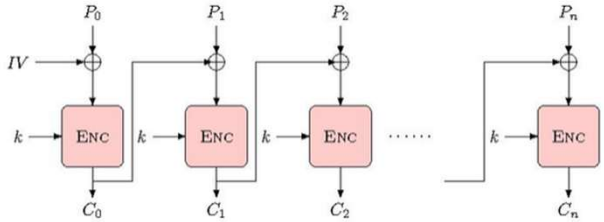
10.5 Symmetric Encryption and Authentication

Page Discussion Read Edit View history Tools

Parent section: [10 Cryptography]

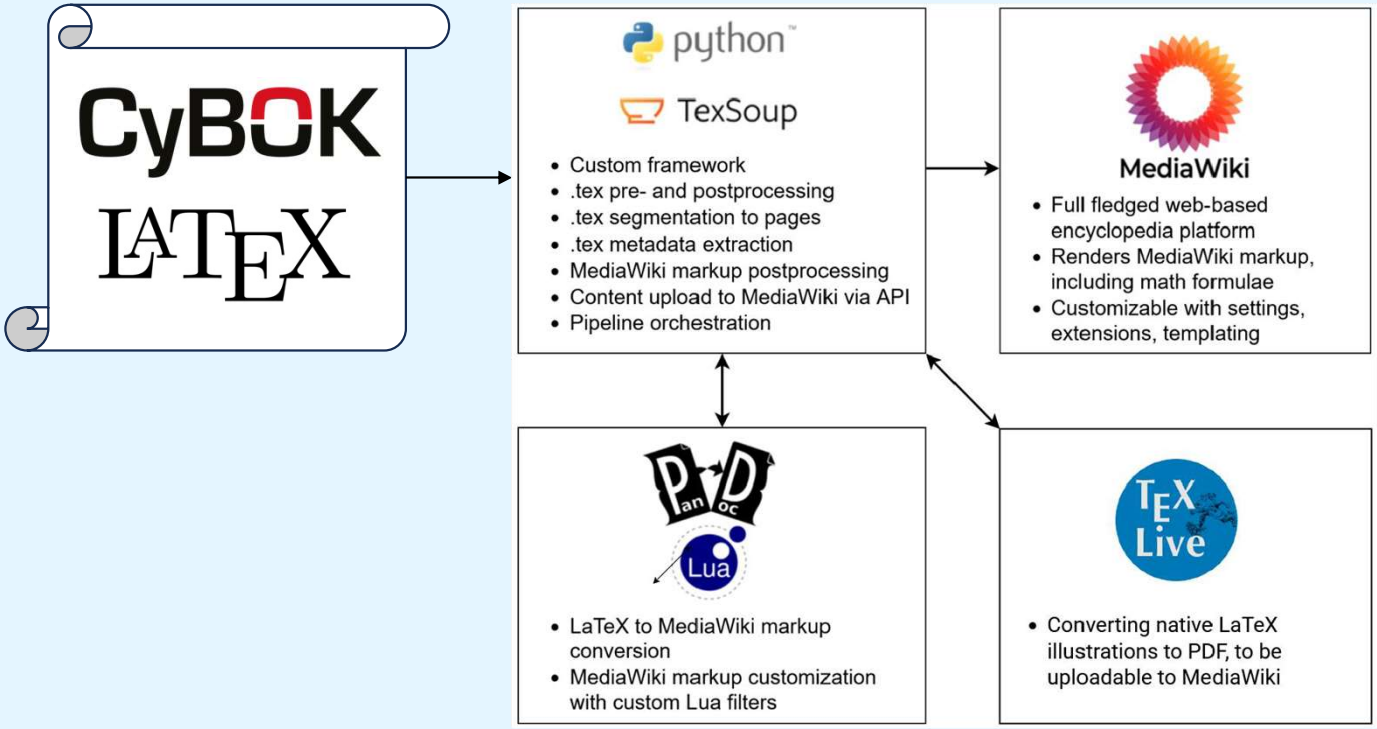
See as PDF

[1][2] A block cipher, such as AES or DES, does not provide an effective form of data encryption or data/entity authentication on its own. To provide such symmetric cryptographic constructions, one needs a scheme, which takes the primitive and then utilizes this in a more complex construction to provide the required cryptographic service. In the context of symmetric encryption, these are provided by modes of operation. In the case of authentication, it is provided by a MAC construction. Additionally, block ciphers are often used to take some entropy and then expand, or collapse, this into a pseudo-random stream or key; a so-called XOF(or Extendable Output Function) or KDF(or Key Derivation Function). Further details on block cipher based constructions can be found at [3], whereas further details on Sponger/Keccak based constructions can be found at [4].



CyBOK

Software proof-of-concept



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

Feasible, but

- Open questions – technical, editorial
- Some technical challenges

- Currently proof of concept
  → lots of work ahead

Some examples...

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

Not all of them make sense as standalone pages:

- Too short

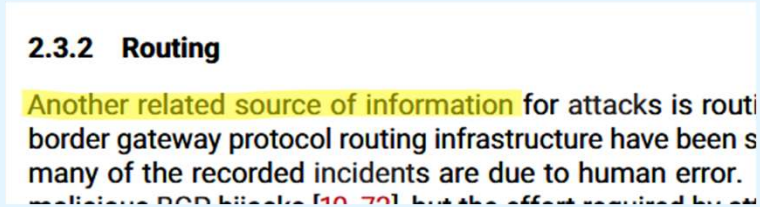
11 OTHER REGULATORY MATTERS

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

- Too context dependent



2.3.2 Routing

Another related source of information for attacks is routi
border gateway protocol routing infrastructure have been s
many of the recorded incidents are due to human error.

Adding Wiki-specific custom LaTeX arguments, including/excluding sections from segmentation

Versioning

- CyBOK as a continuously evolving resource
- Retaining older versions of CyBOK in Wiki
  - So external links, references pointing to it don't break
  - URL namespacing
- Maintaining a timeline of pages
  - In PDF: this happens on KA level
  - **In Wiki: could happen on (sub)section level?**
- Problems:
  - Changes in KA structure
  - Changes in (sub)section titles
  - Diverging/converging (sub)sections
- Related field:
  Ontology versioning

Network Security Knowledge Area
Issue 1.0

Sanjay Jha | University of New South Wales

Network Security Knowledge Area
Version 2.0.0

Christian Rossow | CISPA Helmholtz Center for Information Security
Sanjay Jha | University of New South Wales

Quality reporting pipeline

- Python – plug in anywhere in the conversion process
- Loosely coupled
- Useful for
  - Wiki development QA
  - As-is QA
  - Basis for regression tests

Duplicate titles across KAs

```
{
    "introduction": [
        "authentication, authorisation & accountability",
        "risk management and governance",
        "web & mobile security",
        "introduction",
        "ai for security",
        "security economics",
        "security and privacy of ai"
    ],
    "authentication": [
        "authentication, authorisation & accountability",
        "web & mobile security"
    ],
...
```

Title comparison: PDF vs Wiki

```
{
    "in_pdf__not_in_wiki": [
        "11 Operating Systems and Virtualisation",
        "11.6 Operating Systems, Hypervisors\u2014what about related areas?",
        "12.1.2 Classes of Vulnerabilities & Threats",
        ...
    ],
    "in_wiki__not_in_pdf": [

        "11 Operating Systems & Virtualisation Security",
        "11.6 Operating Systems, Hypervisors---what about related areas?",
        "12.1.2 Classes of Vulnerabilities  \\&  Threats",
        ...
    ]
}
```

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

- How to display section titles?
- LaTeX metadata to MediaWiki

Next steps

- ~~Feasibility study on all 22 Kas~~
- 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.
- Implementation
  - Systemic review of the whole codebase
  - Iterative feedback loop with stakeholders

Thank you!

Lőrinc Thurnay *(Lawrence)*
research associate
Department for E-Governance and Administration

thurnay@protonmail.com

University for Continuing Education Krems

DONAU UNIVERSITÄT KREMS

CyBOK Wiki: feasibility study Documentation

Lőrinc Thurnay | University for Continuing Education Krems

To be updated when new report is released

https://www.cybok.org/media/d Wiki_feasibility_study_finalreport.pdf

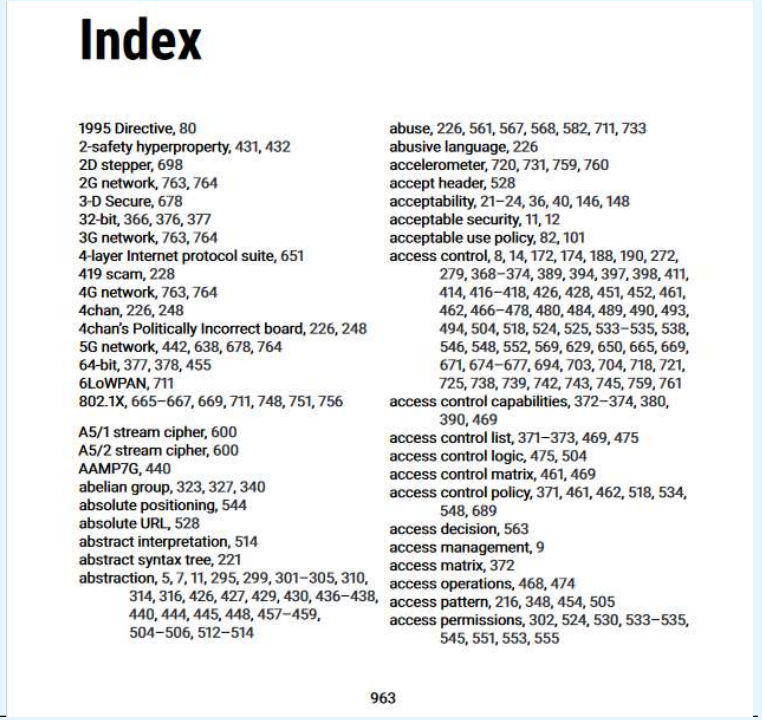
CyBOK

Opportunities and questions

CyBOK is linked with indices, acronyms, glossary

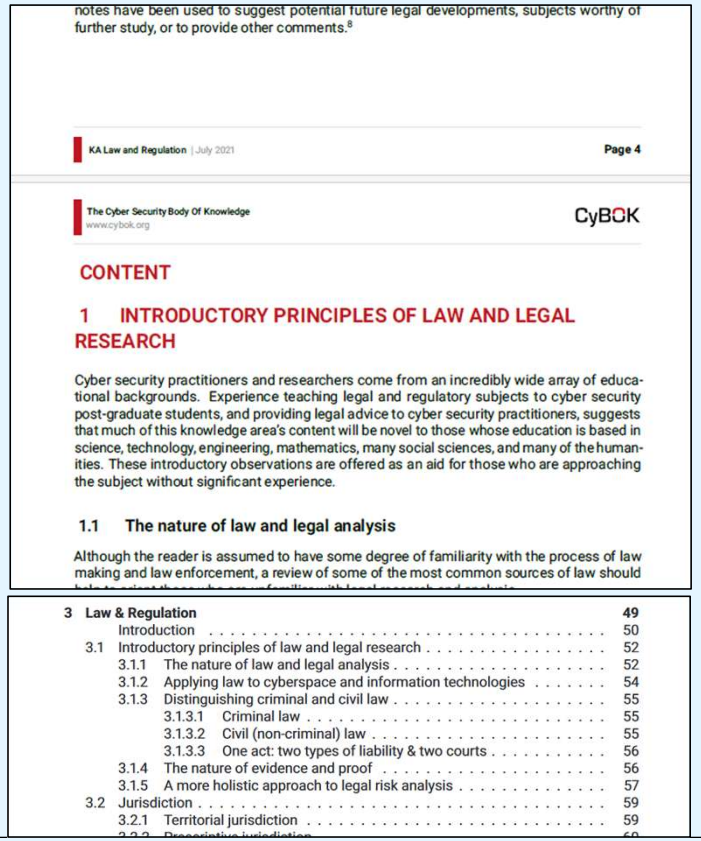
- 2757 `\index{}` elements in one KA
- Opportunities?
  - Dedicated pages, with backlinks
  - recommendations,
  - smart search,
  - topic browser

CyBOK is linked data.



Index

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
www.cybok.org

CyBOK

CONTENT

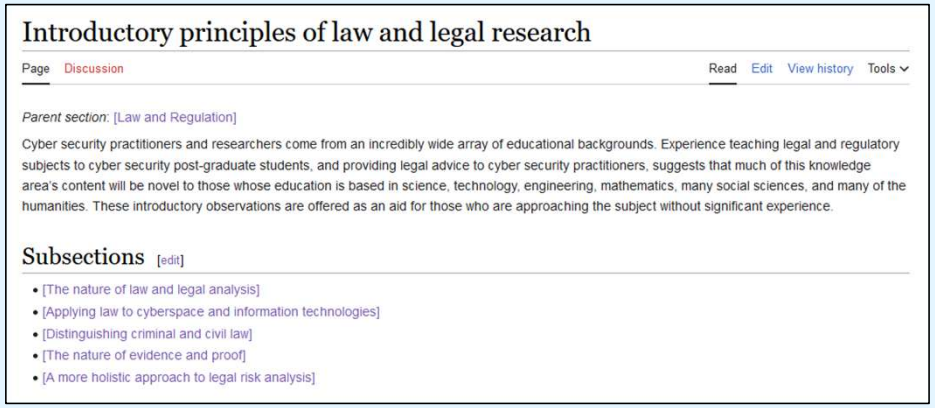
1 INTRODUCTORY PRINCIPLES OF LAW AND LEGAL RESEARCH

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]

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"...