1. Linking with CyBOK Knowledge Areas

The categories were then assigned to their most relevant CyBOK knowledge area, as discussed previously. Categories not included in the list were not assigned a knowledge area.

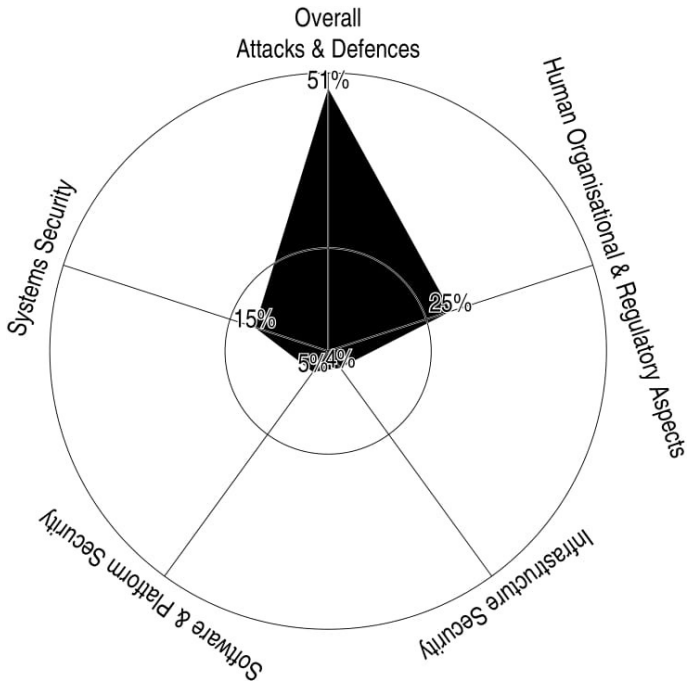
Knowledge Area	Category
Adversarial Behaviour	Carding
Adversarial Behaviour	Cashing Out
Adversarial Behaviour	Clearing Criminal History
Adversarial Behaviour	Counterfeit Currency
Adversarial Behaviour	Denial of Service
Adversarial Behaviour	Doxing
Adversarial Behaviour	eWhoring
Adversarial Behaviour	Fraud
Adversarial Behaviour	Hacking – General
Adversarial Behaviour	Hacking – Malware Supply Chain
Adversarial Behaviour	Modifying Credit
Adversarial Behaviour	Resources – Contact Lists
Adversarial Behaviour	Resources – Identity Documents
Adversarial Behaviour	SEO
Cryptography	Cryptocurrency – General
Cryptography	Cryptocurrency – Trading
Cryptography	PGP/GPG
Forensics	Digital Forensics
Malware & Attack Technologies	Malware Authorship
Network Security	Hacking – Wireless Networks
Physical Layer Security	Hacking – Phreaking
Physical Security	Lockpicking
Physical Security	Weaponry & Explosives
Privacy & Online Rights	Anonymity – Other
Privacy & Online Rights	Anonymity – Proxies
Privacy & Online Rights	Anonymity – Tor
Privacy & Online Rights	Anonymity – VPN
Web and Mobile Security	Hacking – Mobile
Web and Mobile Security	Hacking – Website

2. Creation of representations

The number of entries for each knowledge area were then summed.

The mappings were created using Postscript code written by Joe with the inputs and settings customised. The output PDF files containing the graphs were then trimmed using online tools to remove unnecessary white space.

2.1 Spider Maps



These were created in order to provide a direct comparison to the spider maps created in the Mirror, Mirror diagram.

2.2 Bar Charts

The following categories (LIST) were not covered by the classifier and are therefore set to zero percent.

3. Analysis

3.0 Against Other Darknet Research
While the study did not test a fixed hypothesis, we speculated that based on previous research that ‘Adversarial Behaviour’ would be the most prominent knowledge area and this did prove to be correct.

We also set out, as a research question, to determine whether there was cyber-security related learning material that was not adequately covered within the scope of CyBOK. To answer this question, our study was unable to find any such material of cyber-security relevance that could not be adequately mapped within the scope of CyBOK. However, this answer cannot be considered fully comprehensive

The categories with the highest prevalence I think can be summarised as firstly methods for obtaining money illegally (‘Carding’, ‘Fraud’), secondly methods for cleaning that money (‘Cashing Out’) and lastly, means to stay anonymous while performing these activities (‘Proxies’, ‘Tor’, ‘VPN’).

The steady increase in topics over time within the forums support previous the conclusion from prior research that the demand for illicit services on the darknet will only increase, certainly in the short-term. However, we have yet to see law enforcement find a consistent and pragmatic method of compromising these websites – if this does happen, it will be interesting to see whether the darknet will adapt to counter these measures or collapse completely.

From a more broader criminal perspective, the prevalence of drug related guides within the crypto-markets listings and forums is interesting as it suggests darknet markets are not only being used to trade illicit drugs (which is well documented) but also methodology for production. This will likely exacerbate the drug problem as guides for difficult to manufacture drugs (such as LSD) become more widely available.

Differing darknet communities

3.1 Differences between forums and market listings
The market listings were the most homogenous, with the vast majority of listings falling under 'Adversarial Behaviour'

It was a similar story for the hacker forums except the knowledge areas 'Web and Mobile Security' and 'Privacy & Online Rights' also show some prevalence, though not nearly as much as the 'Adversarial Behaviour' knowledge area.

The crypto-market forums had even more variety, with the 'Privacy & Online Rights' and 'Cryptography' knowledge areas also having similar prevalence.

The focus within Cryptography is largely discussion around PGP, in particular how to use PGP. This is not particularly surprising when you factor in that communication between buyers and sellers on crypto-markets is typically encrypted using PGP. Therefore there are many threads on the crypto-market forums featuring first-time users discussing whether they are encrypting their communication correctly.

The 'Privacy & Online Rights' knowledge area is primarily comprised of discussion around technical methods for avoiding detection, particularly proxies or VPN services. The high demand for this suggests the methodology may become increasingly sophisticated in future to meet these demands.

3.2 Differences over time

Listings
The market listing data is not dated thereby making analysis over time for this dataset impossible.

However previous research into market listings suggest...

Cryptomarket Forums
The crypto-market forum data spans from 2012 to July 2015.

Knowledge Area	**2012**	**2013**	**2014**	**2015***
Attacks & Defences	0.357	0.239	0.357	0.395
Systems Security	0.286	0.397	0.225	0.202
Infrastructure Security	0.036	0.013	0.036	0.049
Human, Organisational & Regulatory Aspects	0.321	0.348	0.371	0.348
Software & Platform Security	0.000	0.003	0.011	0.006

*Until July

Looking at the data, there was no immediately obvious trend with each knowledge area remaining relatively stable over time.

Below is table of the total titles for each year:

Knowledge Area	2012	2013	2014	2015*
Attacks & Defences	10	250	1013	381
Systems Security	8	416	639	195
Infrastructure Security	1	14	102	47
Human, Organisational & Regulatory Aspects	9	364	1053	335
Software & Platform Security	0	3	31	6
Totals	**28**	**1047**	**2838**	**964**

*Until July

The table shows a significant increase in titles year on year, supporting previous research suggesting that the user base of the darknet will continue to grow in size.

Hacker Forums

The number of titles has increased (note that 2018 only contains data for the first two months) though not consistently, it dips from 2014 to 2016.

Knowledge Area	2011	2012	2013	2014	2
Attacks & Defences	0.18	0.34	0.36	0.34	0
Systems Security	0.00	0.00	0.01	0.04	0
Infrastructure Security	0.00	0.03	0.02	0.02	0
Human, Organisational & Regulatory Aspects	0.07	0.29	0.28	0.41	0
Software & Platform Security	0.75	0.34	0.33	0.18	0

The percentage of titles relating to Attacks & Defences increased almost year-on-year, rising from 18% in 2011 to 68% in 2017. The consistent growth in this area over many years suggests this trend will continue in future and that cyber-security curricula need to be well prepared to counter that demand.

The ‘Software & Platform Security’ category showed the exact inverse trend, starting at 75% in 2011 until 10% in 2017.

One potential reason for this trend could be greater awareness of and greater accessibility to these darknet forums. An increase of less technically minded users could explain the increase in get-rich-quick-type categories (such as Carding and Fraud) over more technically minded categories (such as Hacking). If this trend continues, it supports the findings of prior darknet research (cite) which suggest the darknet is likely to grow significantly in the following years.

‘Infrastructure Security’ remained at zero to very low levels throughout, suggesting this was never a key area of interest for their user base.

3.3 Comparison with mappings of cyber-security curricula (Mirror, Mirror study)

What the Mirror, Mirror study concluded

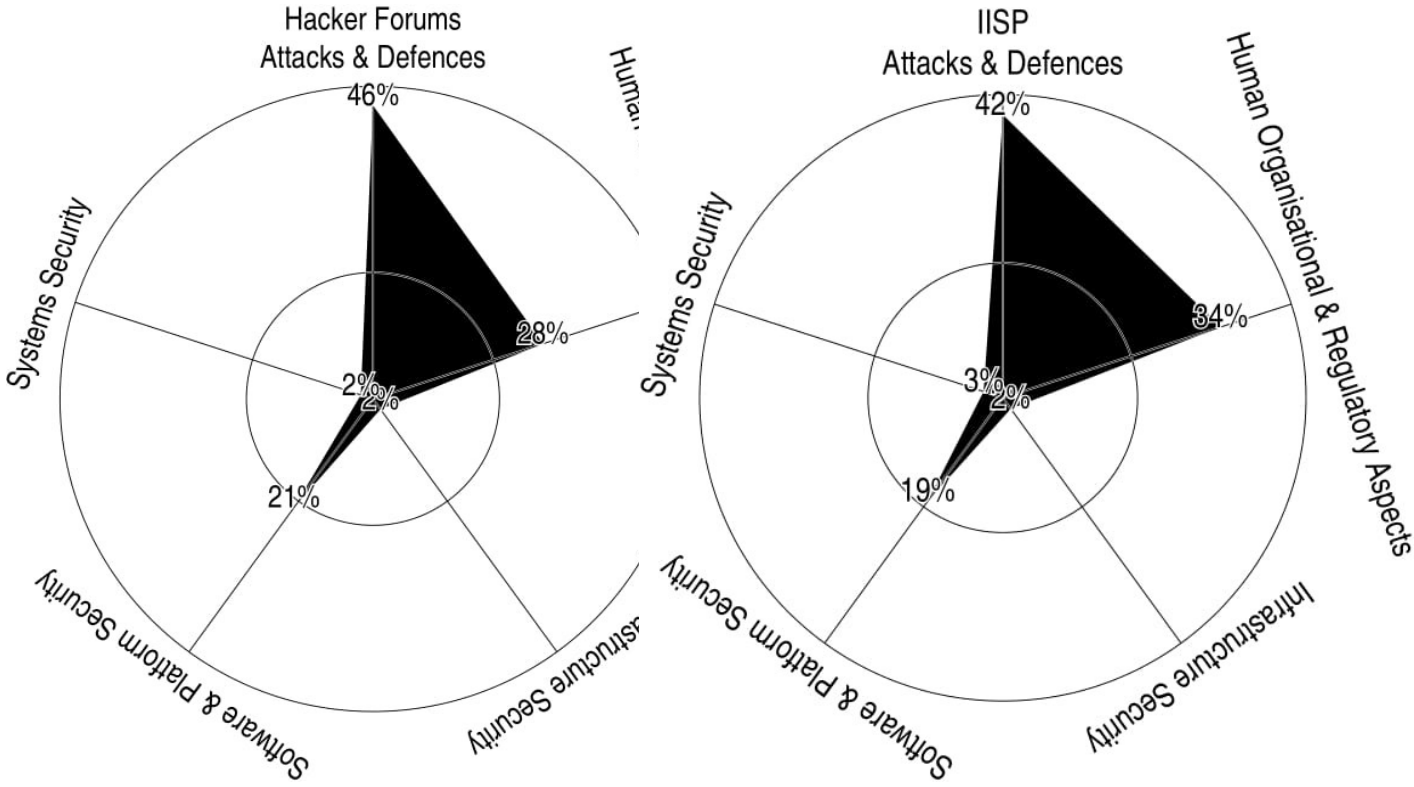
- The Mirror, Mirror study identified that the curriculums of cyber-security qualifications differed considerably in their content and found some to be particularly narrow in scope.
- In addition, every curriculum appeared to lack coverage of some cyber-security knowledge areas.

How our study can build upon it to add value
Our study can add a further perspective by determining whether the weightings of these curricula are proportionate to the available demand

- The most clear difference between the mappings created in the Mirror, Mirror study versus the mappings created through analysis of learning material on the darknet is that, perhaps unsurprisingly, is there is that there is generally more variability across the knowledge areas.
- This is understandable as all the courses are supposed to be generalist and intended to cover a wide variety of topics

Similarities between Hacker set and IISP
The mapping of the hacker forum dataset and the IISP shares many similarities.

Fig 1 & 2. Hacker Forums comparison with IISP



- While this was suspected as being deficient, this research suggests this particular curriculum is effectively covering the material available on the hacker forums.

It should be noted that the focus differs within these broader knowledge areas. For example, within the Human & Organisational knowledge areas the focus is primarily on Risk Management & Governance whereas the hacker forums is entirely focussed on Privacy & Online Rights.

- Users on hacker forums are primarily interested in tools related to ‘target hardening’ capabilities, making them more difficult to track (i.e. proxies, VPNs, Tor etc.)
- While there is no doubt a need for qualifications to teach a basic understanding of these, they are of more use to those engaging in hacking activities as opposed to those intending to trace them (proactive vs. reactive)

- As far as I am aware there is not a practical system that can compromise these technologies as yet (?), so cannot be taught on a course.

Similarly, within ‘Attacks and Defences’ IISP focuses primarily on ‘Security Operations & Incident Management’ whereas the hacker forum emphasis is on ‘Adversarial Behaviour’

- It could be argued this is unsurprising as ‘Adversarial Behaviours’ largely features methods used by those attacking systems while ‘Security Operations & Incident Management’ comprises the methodology for securing those systems.
- There is little demand for SOIM content on the darknet as most users are more interested in breaking into these systems rather than defending them.

Adversarial Behaviour - Differences

Another clear difference is that the knowledge area ‘Adversarial Behaviour’ which features disproportionately in the darknet learning material, in contrast, is severely under represented in every cyber-security accreditation.

- With this in mind, it may be worth increasing the presence of this knowledge area within these accreditations in order to reflect the disproportionate demand on the darknet.
- In addition, the mappings over time suggest that this knowledge area will only increase over time.

It is worth mentioning that much of the content within the Adversarial Behaviour knowledge area is concentrated within the activities of carding and cashing out.

- The increasingly high levels of carding and money laundering related learning materials suggest that any measures that are being taught to curb these are ineffective.
- In addition, it suggests the introduction of bitcoin and bitcoin mixers suggest money laundering has been made substantially easier to conduct and harder to detect
- Taking this into account, it may be worth creating a specific qualification for those working in the banking sector.

Privacy and Online Rights - Differences

‘Privacy & Online Rights’ features somewhat prominently within the learning material, particularly the crypto-market forums where there is a lot of discussion relating to proxies, VPNs and the TOR browser.

- Focus is on defensive tools to stay anonymous while engaging in illicit activity.
- Cyber-security curricula focus is generally on ‘Risk Management and Governance’ which refer to security management systems

Software and Platform Security

KAs that relate entirely to the development of software, such as Secure Software Lifecycle, are virtually non-existent within the dataset.

- Users on the hacker and crytpomarket forums are generally disinterested in legitimate software development or at least, discussing it on the darkweb.
- There is more of a focus within the cyber-security qualifications
- However, there are a large amount of technical e-books on the market listings, some of which relate to software development.

Infrastructure Security – Commonality (Low Prevalence)

A commonality between all the cyber-security curricula and darknet learning material is the low prevalence of infrastructure security. This is particularly evident in the hacker forum dataset where there are almost no instances of titles relating to infrastructure security.

- This would suggest that the reason this area does not feature more prominently in cyber-security curricula is that there is not a sufficient threat to warrant the demand.
- It should also be noted some of the categories are positioned in a way that bit generous in regards to physical security so the actual prevalence of relevant cyber-physical security items is likely lower than. For example, ‘Weapons & Explosives’ encompasses firearms which could be for personal protection rather than for breaking into a building.
- This is not to say we should be remiss about infrastructure security – there may be a need for a niche qualification which focusses on this but this research does not support the idea that infrastructure security should be given equal weighting with the other knowledge areas for a general cyber-security qualification.
- Worth noting that since certain areas like hardware security are so niche within cyber-security, a hacker with an expertise in this area will be particularly dangerous.

Teaching Methodology to Implement

Previous research (All-That-Glitters) into cyber-security qualifications has determined they often rely heavily on ineffective techniques such as multiple choice examinations.
Therefore, once these deficits are identified, they should not only be remedied in terms of emphasis but also using one of the proposed cost-effective methodology identified in the study, such as via oral examination.

General Suggestions

- Many of these Kas are quite exclusive with little crossover, some as well do not seem to have the threat to warrant the demand (thought should not be ignored)
- Maybe a good idea to have more specified qualifications to cater to particular areas.