There is a major recruitment crisis within the cybersecurity industry [1]; yet at the same time there is an active community of people with an interest in hacking and cybersecurity who interact with each other through online forums and offline conventions.

Conversations held within these settings cover the full range of hacking activities and attitudes from overtly criminal (black hat) to purely ethical (white hat) activities, and all of the variations in-between (grey hat).

Online forums may be the first contact that young people with an interest in computing have with the hacking world, as such it is important to better understand the beliefs, attitudes and group dynamics that they experience and the influence that this has.

Through engaging with these communities we can encourage individuals to pursue the many legitimate careers in cybersecurity where they can follow their passions, and in doing help address the cybersecurity jobs gap.

Linguistic Inquiry Word Count (LIWC) analysis

LIWC software was used to analyse each forum/subreddit on four measure of analytical thinking, clout, authenticity and emotional tone:

- Analytical thinking reflects the degree to which individuals demonstrate formal, logical and hierarchical thinking patterns
- Clout is a measure of the relative social status, confidence and leadership that individuals display through their writing
- Authenticity measures the degree to which people are using language that indicates they are being more personal, honest and vulnerable
- Emotional tone indicates the degree to which positive and negative emotions are evident in the text, with a score below 50 suggesting a more negative emotional tone

<table>
<thead>
<tr>
<th></th>
<th>Word count</th>
<th>Analytic</th>
<th>Clout</th>
<th>Authentic</th>
<th>Tone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forum 1</td>
<td>8595</td>
<td>33.1</td>
<td>55.59</td>
<td>43.84</td>
<td>51.92</td>
</tr>
<tr>
<td>Forum 2</td>
<td>11112</td>
<td>41.73</td>
<td>62.34</td>
<td>52.85</td>
<td>62.96</td>
</tr>
<tr>
<td>Forum 3</td>
<td>24986</td>
<td>47.98</td>
<td>52.9</td>
<td>44.7</td>
<td>45.7</td>
</tr>
<tr>
<td>Forum 4</td>
<td>19014</td>
<td>54.4</td>
<td>59.89</td>
<td>29.97</td>
<td>44.03</td>
</tr>
<tr>
<td>Subreddit 1</td>
<td>14116</td>
<td>54.78</td>
<td>60.41</td>
<td>47.9</td>
<td>55.84</td>
</tr>
<tr>
<td>Subreddit 2</td>
<td>25104</td>
<td>53.18</td>
<td>56.78</td>
<td>31.41</td>
<td>58.78</td>
</tr>
<tr>
<td>Subreddit 3</td>
<td>15687</td>
<td>51.98</td>
<td>64.98</td>
<td>31.14</td>
<td>47.97</td>
</tr>
</tbody>
</table>

Note the closer the score is to 100 the greater the presence of that variable in the text.

Thematic analysis

An initial, exploratory thematic analysis procedure was used, following Braun & Clarke (2006). The following interconnected themes were identified:

- Skill acquisition
- Honesty
- Knowledge
- Legality
- Risk
- Legitimacy

Discussion

As demonstrated by the LIWC analysis there variation evident in the language style and psychological processes used within different sites. Overall the online discussions were characterised by high levels of clout, indicating that users exhibit confidence and preference towards social status and leadership. This was consistent was the themes of knowledge and skill acquisition, which suggested that the intellectual challenges of hacking are a powerful motivator for individuals to become involved in this activity. This is consistent with proposed typologies of hacker identity [5]. Throughout the analysis there was a strong awareness of the potential illegality and risks of hacking. It should be noted that in the majority of cases, albeit not all, any expression of intent to commit a potential illegal activity was condemned by members of the community. However opinions and beliefs around the grey hat areas were more subtle and complex. There was a clear passion and skillset amongst the majority of users to make systems better and more secure. Harnessing this knowledge may help society address cybersecurity challenges.

References